Installationshandbuch
Revision B

McAfee® Email Gateway 7.x – Blade Servers

COPYRIGHT
Copyright © 2013 McAfee, Inc. Keine Vervielfältigung ohne vorherige Zustimmung.

MARKEN
McAfee, das McAfee-Logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq sind Marken oder eingetragene Marken von McAfee, Inc. oder der Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.

INFORMATIONEN ZUR LIZENZ

Lizenzvereinbarung
HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Einleitung **5**

Informationen zu diesem Handbuch 5
Zielgruppe 5
Konventionen 5
Verwendung dieses Handbuchs 7
Quellen für Produktinformationen 7

1 Vorbereitung der Installation **9**

Lieferumfang 9
Planen der Installation 10
Nicht bestimmungsgemäße Nutzung 11
Betriebsbedingungen 11
Positionieren des Blade-Servers 11
Überlegungen zu Netzwerkmodi 11
Modus "Transparente Bridge" 12
Modus "Transparenter Router" 15
Modus "Expliziter Proxy" 17
Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ 19
SMTP-Konfiguration in einer DMZ 19
Arbeitslastverwaltung 21

2 Anschließen und Konfigurieren des Blade-Servers **23**

Upgrades von früheren Versionen 24
Konfigurieren der Interconnect-Module bei der Aktualisierung von einer älteren Version . . 24
Sichern der vorhandenen Konfiguration 25
Herunterfahren der Scan-Blades 25
Herunterfahren der Management-Blade-Server 26
Upgrade der Software für den Management-Blade-Server 26
Erneute Installation der Scan-Blades 27
Standardinstallation 28
Montieren des Blade-Servers 29
Installieren der Interconnect-Module für den Standardmodus (nicht ausfallsicher) 29
Anschließen des Blade-Servers an das Stromnetz 31
Verbindung mit dem Netzwerk 32
Installieren der Software 34
Installationsreihenfolge der Management-Blade-Server 34
Installation der Software auf den Management-Blade-Servern 35
Installieren der Software auf einem Blade-Server zum Scannen von Inhalten 36
Verwenden der Konfigurationskonsole 36
Durchführen der benutzerdefinierten Einrichtung 37
Wiederherstellung aus einer Datei 37
Setup im Modus 'Nur Verschlüsselung' 37

3 Vorstellung des Dashboards **39**

Das Dashboard 39

Vorteile der Verwendung des Dashboards . . . 40
Dashboard-Portlets . . . 41
Vorgehensweise – Deaktivieren des Warnhinweises *McAfee Global Threat Intelligence-Feedback deaktiviert* . . . 42
Funktionen des Blade-Servers . . . 42
Demonstrieren der Failover- und Arbeitslastverwaltung . . . 42
Testen der Verwaltungsfunktionen auf dem Blade-Server . . . 43
Verwenden von Richtlinien für die Verwaltung von Nachrichten-Scans . . . 45
Testen der Konfiguration . . . 50
Erkunden der McAfee Email Gateway Blade Server-Funktionen . . . 51

4 Betrieb im ausfallsicheren Modus 55
Nutzung der Hardware im ausfallsicheren Modus . . . 56
Entscheidung für die Verwendung des ausfallsicheren Modus . . . 57
Vor dem Umkonfigurieren in den ausfallsicheren Modus . . . 58
Hardware-Informationen . . . 58
Für den ausfallsicheren Modus erforderliche IP-Adressen . . . 59
Benutzernamen und Kennwörter . . . 60
Aktivieren des ausfallsicheren Modus . . . 61
Sichern der vorhandenen Konfiguration . . . 62
Installieren der Interconnect-Module für den ausfallsicheren Modus . . . 62
Konfigurieren der Interconnect-Module . . . 64
Ändern der Gehäusekonfiguration . . . 66
Anwenden der Konfiguration für den ausfallsicheren Modus auf alle Interconnect-Module . . . 68
Herunterladen und Überprüfen der generierten Konfiguration . . . 69
Konfigurieren des Management-Blade-Servers für den ausfallsicheren Modus . . . 69
Verbindungen zum externen Netzwerk im ausfallsicheren Modus . . . 70
Einschalten der Blades . . . 72

5 Fehlerbehebung 73
Blade-spezifische Fehlerbehebung . . . 73
Externe Überwachungssysteme . . . 73
Status der Netzwerkkarte . . . 73
Systemereignisse . . . 73

A Anhänge 75
Beispiel für die Basiskonfiguration eines Interconnect-Moduls . . . 75
Beispiel einer Chassis-Konfigurationsdatei . . . 76
Prozeduren für den Hardware-Austausch . . . 78
Ersetzen eines ausgefallenen Management-Blade-Servers . . . 78
Ersetzen eines ausgefallenen Failover-Management-Blade-Servers . . . 79
Ersetzen eines ausgefallenen Blade-Servers zum Scannen von Inhalten . . . 79
Ersetzen eines ausgefallenen Interconnect-Moduls . . . 79
Ersetzen eines ausgefallenen Onboard-Administrator-Moduls . . . 80

Index 81

Einleitung

Dieses Handbuch enthält die Informationen, die Sie zum Installieren Ihres McAfee-Produkts benötigen.

Inhalt

- *Informationen zu diesem Handbuch*
- *Quellen für Produktinformationen*

Informationen zu diesem Handbuch

In diesem Abschnitt werden die Zielgruppe des Handbuchs, die verwendeten typografischen Konventionen und Symbole sowie die Gliederung des Handbuchs beschrieben.

Zielgruppe

Die Dokumentation von McAfee wird inhaltlich sorgfältig auf die Zielgruppe abgestimmt.

Die Informationen in diesem Handbuch richten sich in erster Linie an:

- **Administratoren** – Personen, die das Sicherheitsprogramm eines Unternehmens implementieren und umsetzen.

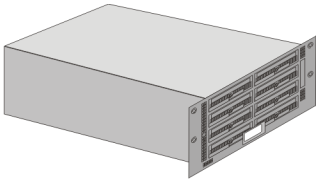
Konventionen

In diesem Handbuch werden folgende typografische Konventionen und Symbole verwendet.

Buchtitel, *Begriff*, *Hervorhebung*	Titel eines Buchs, Kapitels oder Themas; ein neuer Begriff; eine Hervorhebung.
Fett	Text, der stark hervorgehoben wird.
`Benutzereingabe, Code, Meldung`	Befehle oder andere Texte, die vom Benutzer eingegeben werden; ein Code-Beispiel; eine angezeigte Meldung.
Benutzeroberflächentext	Wörter aus der Benutzeroberfläche des Produkts, z. B. Optionen, Menüs, Schaltflächen und Dialogfelder.
Hypertext-Blau	Ein Link auf ein Thema oder eine externe Website.
	Hinweis: Zusätzliche Informationen, beispielsweise eine alternative Methode für den Zugriff auf eine Option.
	Tipp: Vorschläge und Empfehlungen.
	Wichtig/Vorsicht: Wichtige Ratschläge zum Schutz Ihres Computersystems, der Software-Installation, des Netzwerks, Ihres Unternehmens oder Ihrer Daten.
	Warnung: Wichtige Ratschläge, um körperliche Verletzungen bei der Nutzung eines Hardware-Produkts zu vermeiden.

Graphische Konventionen

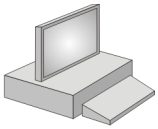
Lernen Sie die grafischen Symbole kennen, die in diesem Dokument verwendet werden.


Blade-Server

Internet oder externe Netzwerke

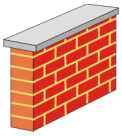
E-Mail-Server

Andere Server (z. B. DNS-Server)


Benutzer- oder Client-Computer

Router

Switch


Firewall

Netzwerkzone (DMZ oder VLAN)

Netzwerk

Tatsächlicher Datenpfad

Wahrgenommener Datenpfad

Definition der Begriffe in diesem Handbuch

Lernen Sie einige der Schlüsselbegriffe kennen, die in diesem Dokument verwendet werden.

Begriff	Beschreibung
Demilitarisierte Zone (DMZ)	Ein Computer-Host oder kleineres Netzwerk, das als Puffer zwischen ein privates Netzwerk und das äußere öffentliche Netzwerk eingefügt wurde, um den direkten Zugriff durch außenstehende Benutzer auf Ressourcen im privaten Netzwerk zu verhindern.
DAT-Dateien	Erkennungsdefinitionsdateien (DAT), auch als Signaturdateien bezeichnet, enthalten die Definitionen, die Viren, Trojaner, Spyware, Adware und andere potenziell unerwünschte Programme (PUPe) identifizieren, erkennen und entfernen.
Betriebsmodus	Es gibt drei Betriebsmodi für das Produkt: "Expliziter Proxy", "Transparente Bridge" und "Transparenter Router".
Richtlinie	Eine Sammlung der Sicherheitskriterien (z. B. Konfigurationseinstellungen, Benchmarks und Spezifikationen für den Netzwerkzugriff), die die erforderliche Compliance-Stufe für Benutzer, Geräte und Systeme definieren, die von einer McAfee-Sicherheitsanwendung bewertet oder erzwungen werden kann.

Begriff	Beschreibung
Reputationsdienst-Prüfung	Teil der Absenderauthentifizierung. Wenn ein Absender die Reputationsdienst-Prüfung nicht besteht, ist die Appliance so eingestellt, dass die Verbindung beendet und die Nachricht nicht zugelassen wird. Die IP-Adresse des Absenders wird zu einer Liste blockierter Verbindungen hinzugefügt und in Zukunft automatisch auf Kernel-Ebene blockiert.
Interconnect-Module	Die HP GbE2c Layer 2/3 Ethernet Blade Switch-Module werden verwendet, um Netzwerkverbindungen zum McAfee Email Gateway Blade Server herzustellen. Der Begriff *Interconnect-Modul* bedeutet dasselbe wie *Switch*.

Verwendung dieses Handbuchs

Dieser Abschnitt enthält eine kurze Zusammenfassung der in diesem Dokument enthaltenen Informationen.

In diesem Handbuch wird Folgendes behandelt:

- Planung und Ausführung Ihrer Installation.
- Umgang mit der Benutzeroberfläche.
- Testen der ordnungsgemäßen Funktion des Produkts.
- Anwendung der aktuellsten Erkennungsdefinitionsdateien.
- Vertrautmachen mit einigen Scan-Richtlinien, Erstellen von Berichten und Abrufen der Statusinformationen.
- Beheben einiger grundlegender Probleme.

Weitere Informationen über die Scan-Funktionen des Produkts finden Sie in der Online-Hilfe des Produkts und in der aktuellen Version des *McAfee Email Gateway-Administratorhandbuches*.

Quellen für Produktinformationen

McAfee stellt Ihnen die Informationen zur Verfügung, die Sie in den einzelnen Phasen der Produktimplementierung benötigen – von der Installation bis hin zur täglichen Nutzung und Fehlerbehebung. Nach der Produktveröffentlichung erhalten Sie Informationen zu diesem Produkt online in der KnowledgeBase von McAfee.

Vorgehensweise

1 Wechseln Sie zum McAfee Technical Support ServicePortal unter http://mysupport.mcafee.com.

2 Greifen Sie unter **Self Service** (Online-Support) auf die erforderlichen Informationen zu:

Zugriff auf	Vorgehensweise
Benutzerdokumentation	1 Klicken Sie auf **Product Documentation** (Produktdokumentation). 2 Wählen Sie ein Produkt und dann eine Version aus. 3 Wählen Sie ein Produktdokument aus.
KnowledgeBase	• Klicken Sie auf **Search the KnowledgeBase** (KnowledgeBase durchsuchen), um Antworten auf Ihre produktbezogenen Fragen zu erhalten. • Klicken Sie auf **Browse the KnowledgeBase** (KnowledgeBase durchblättern), um Artikel nach Produkt und Version aufzulisten.

1 Vorbereitung der Installation

Um den sicheren Betrieb Ihrer McAfee Email Gateway Blade Server zu gewährleisten, sollten Sie folgende Punkte vor Beginn der Installation bedenken.

- Lernen Sie die stromtechnischen Anforderungen Ihres Blade-Servers und Ihres Stromversorgungssystems kennen.
- Machen Sie sich mit den Betriebsmodi und den Funktionen vertraut. Es ist wichtig, dass Sie eine gültige Konfiguration auswählen.
- Entscheiden Sie, wie Sie die Appliance in Ihr Netzwerk integrieren möchten, und stellen Sie fest, welche Informationen Sie benötigen, bevor Sie beginnen. Sie benötigen beispielsweise den Namen und die IP-Adresse des Geräts.
- Packen Sie das Produkt so nah wie möglich am vorgesehenen Aufstellungsort aus.

  Der Blade-Server ist schwer. Beachten Sie beim Auspacken die folgenden Empfehlungen für das Heben des Blade-Servers.

- Nehmen Sie das Produkt aus der Schutzverpackung, und stellen Sie es auf eine ebene Fläche.
- Beachten Sie alle Sicherheitswarnungen.

  Lesen Sie alle mitgelieferten Sicherheitsinformationen, und machen Sie sich mit ihnen vertraut.

Inhalt

- *Lieferumfang*
- *Planen der Installation*
- *Nicht bestimmungsgemäße Nutzung*
- *Betriebsbedingungen*
- *Positionieren des Blade-Servers*
- *Überlegungen zu Netzwerkmodi*
- *Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ*

Lieferumfang

Stellen Sie mithilfe dieser Informationen sicher, dass die Lieferung des Produkts vollständig ist.

Überprüfen Sie anhand der mit dem Produkt ausgelieferten Packliste, ob alle Komponenten enthalten sind.

Folgendes sollte vorhanden sein:

- Ein Blade-Server-Gehäuse
- Ein Management-Blade-Server

- Ein Failover-Management-Blade-Server
- Ein oder mehrere Scan-Blades, abhängig von der Bestellung
- Netzkabel
- Netzwerkkabel
- Installations- und Wiederherstellungs-CD für McAfee Email Gateway
- CD mit dem Linux-Quellcode

Wenn ein Element fehlt oder beschädigt ist, setzen Sie sich mit dem Händler in Verbindung.

Planen der Installation

Nutzen Sie diese Informationen, um die Installation des Geräts zu planen.

Bevor Sie den McAfee Email Gateway Blade Server auspacken, sollten Sie unbedingt die Installation und Ausbringung planen.

Informationen hierzu finden Sie im: HP BladeSystem c-Class Site Planning Guide.

Beachten Sie Folgendes:

- Allgemeine Richtlinien zum Vorbereiten Ihres Standorts.

  Übersichten über die allgemeinen Anforderungen an den Standort zur Vorbereitung Ihres Computer-Raums für die McAfee Email Gateway Blade Server-Hardware.

- Umgebungsanforderungen

  Informationen zu den Umgebungsanforderungen, einschließlich Temperatur, Belüftung und Platzbedarf.

- Stromanforderungen und Überlegungen

  Stromanforderungen und elektrische Faktoren, die vor der Installation bedacht werden müssen.

  Umfasst die Installation der Power Distribution Unit (PDU).

- Hardware-Spezifikationen und -Anforderungen

  Systemspezifikationen für das Blade-Server-Gehäuse, Racks und einphasige und dreiphasige Stromquellen.

- Konfigurationsszenarien
- Vorbereiten der Installation

Nicht bestimmungsgemäße Nutzung

Erfahren Sie, wie Sie vermeiden, das Produkt nicht bestimmungsgemäß zu nutzen.

McAfee Email Gateway Blade Server ist:

- **Keine Firewall** – Es muss in Ihrer Organisation hinter einer ordnungsgemäß konfigurierten Firewall verwendet werden.
- **Kein Server zum Speichern zusätzlicher Software und Dateien** – Installieren Sie keine Software auf dem Gerät, und fügen Sie keine zusätzlichen Dateien hinzu, es sei denn, Sie werden in der Produktdokumentation oder von Ihrem Support-Mitarbeiter dazu aufgefordert.

Das Gerät kann nicht alle Arten von Datenverkehr verarbeiten. Wenn Sie den Modus „Expliziter Proxy" verwenden, sollten nur Protokolle an das Gerät gesendet werden, die gescannt werden müssen.

Betriebsbedingungen

In diesem Abschnitt lernen Sie die Umgebungsbedingungen kennen, die für das McAfee Email Gateway erforderlich sind.

Betriebstemperatur	+10 °C bis + 30 °C oder +10 °C bis + 35 °C (modellabhängig), wobei die Änderungsgeschwindigkeit maximal 10 °C pro Stunde beträgt
Lagerungstemperatur	-40 °C bis +70 °C
Relative Feuchtigkeit bei Lagerung	90 %, nicht kondensierend bei 35 °C
Vibration, unverpackt	5 Hz bis 500 Hz, 2,20 g RMS regellos
Erschütterung, im Betrieb	Halbsinus, 2 g Höchstwert, 11 m/Sek
Erschütterung, unverpackt trapezoid	25 g, Geschwindigkeitsänderung 3,45 m/Sek. (≧18,1 kg bis > 36,3 kg)
Kühlbedarf des Systems in Watt	486,38 W oder 747,15 W (modellabhängig)

Positionieren des Blade-Servers

In diesem Abschnitt erfahren Sie, wo der McAfee Email Gateway Blade Server positioniert werden sollte.

Installieren Sie den Blade-Server so, dass Sie den physischen Zugang zur Einheit steuern und auf die Anschlüsse und Verbindungen zugreifen können.

Mit dem Chassis des Blade-Servers wird ein Set zur Montage in einem Rack ausgeliefert, mit dem Sie den Blade-Server in einem 19-Zoll-Rack installieren können.

Unter HP BladeSystem c7000 Enclosure Quick Setup Instructions.

Überlegungen zu Netzwerkmodi

In diesem Abschnitt lernen Sie die Betriebsmodi (Netzwerkmodi) kennen, in denen das Gerät betrieben werden kann.

Bevor Sie den McAfee Email Gateway Blade Server installieren und konfigurieren, müssen Sie sich überlegen, welchen Netzwerkmodus Sie verwenden möchten. Vom ausgewählten Modus hängt es ab, wie Sie Ihre Appliance physisch an Ihr Netzwerk anschließen.

Sie können einen der folgenden Netzwerkmodi auswählen:

- **Modus "Transparente Bridge"** – Das Gerät fungiert als Ethernet-Bridge.
- **Modus "Transparenter Router"** – Das Gerät fungiert als Router.
- **Modus "Expliziter Proxy"** – Das Gerät fungiert als Proxyserver und Mail-Relay.

Wenn Sie nach der Lektüre dieses und der folgenden Abschnitte weiterhin unsicher sind, welchen Modus Sie verwenden sollen, sprechen Sie mit einem Netzwerkexperten.

Architektonische Aspekte hinsichtlich der Netzwerkmodi

Hinsichtlich der Netzwerkmodi müssen Sie vor allem folgende Aspekte bedenken:

- Ob Kommunikationsgeräte die Existenz des Geräts kennen. Das heißt, ob das Gerät in einem der transparenten Modi arbeitet.
- Wie das Gerät physisch mit Ihrem Netzwerk verbunden wird.
- Die erforderliche Konfiguration zur Integration des Geräts in Ihr Netzwerk.
- An welchem Ort im Netzwerk die Konfiguration erfolgt.

Überlegungen vor dem Ändern des Netzwerkmodus

In den Modi "Expliziter Proxy" und "Transparenter Router" können Sie das Gerät so einrichten, dass es sich innerhalb mehrerer Netzwerke befindet. Dies wird durch das Einrichten mehrerer IP-Adressen für die LAN1- und LAN2-Anschlüsse ermöglicht.

Wenn Sie aus dem Modus "Expliziter Proxy" oder "Transparenter Router" in den Modus "Transparente Bridge" wechseln, wird nur die aktivierte IP-Adresse für jeden Anschluss übernommen.

Nachdem ein Netzwerkmodus festgelegt wurde, empfiehlt es sich, diesen nicht mehr zu ändern, es sei denn, der Standort des Geräts ändert sich oder das Netzwerk wird neu strukturiert.

Modus "Transparente Bridge"

In diesem Abschnitt lernen Sie den Modus "Transparente Bridge" des McAfee Email Gateways besser kennen.

Im Modus "Transparente Bridge" bemerken die kommunizierenden Server das Gerät nicht. Der Betrieb des Geräts ist für die Server transparent.

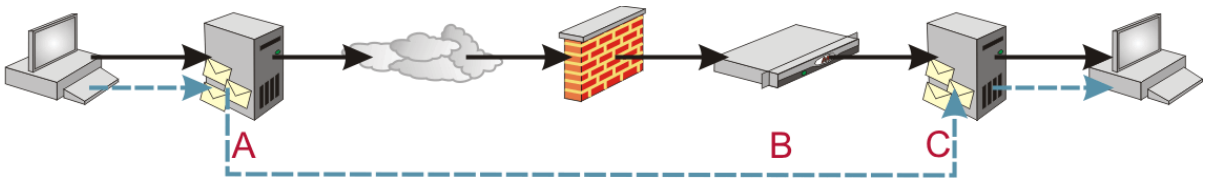


Abbildung 1-1 Modus "Transparente Bridge" – sichtbarer Datenpfad

In der Abbildung sendet der externe E-Mail-Server (**A**) E-Mail-Nachrichten an den internen E-Mail-Server (**C**). Der externe Mail-Server kann nicht erkennen, dass die von ihm gesendete E-Mail-Nachricht vom Gerät abgefangen und gescannt wird (**B**).

Der externe E-Mail-Server scheint direkt mit dem internen E-Mail-Server zu kommunizieren (der Pfad wird als gestrichelte Linie dargestellt). Tatsächlich wird der Datenverkehr möglicherweise durch mehrere Netzwerkgeräte geleitet und vom Gerät abgefangen und gescannt, bevor er den internen Mail-Server erreicht.

Arbeitsweise des Geräts im Modus "Transparente Bridge"

Im Modus "Transparente Bridge" wird das Gerät über den LAN1- und den LAN2-Anschluss mit dem Netzwerk verbunden. Das Gerät scannt den empfangenen Datenverkehr und fungiert als Bridge, die zwei Netzwerksegmente verbindet, behandelt diese aber wie ein einziges logisches Netzwerk.

Konfiguration im Modus "Transparente Bridge"

Der Modus "Transparente Bridge" erfordert weniger Konfigurationsaufwand als die Modi "Transparenter Router" oder "Expliziter Proxy". Sie müssen nicht alle Clients, das Standard-Gateway, MX-Einträge, Firewall-NAT und E-Mail-Server neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Da das Gerät in diesem Modus nicht als Router fungiert, ist es auch nicht erforderlich, eine Routing-Tabelle zu aktualisieren.

Platzieren des Geräts bei Betrieb im Modus "Transparente Bridge"

Aus Sicherheitsgründen sollten Sie das Gerät innerhalb Ihres Unternehmens und hinter einer Firewall betreiben.

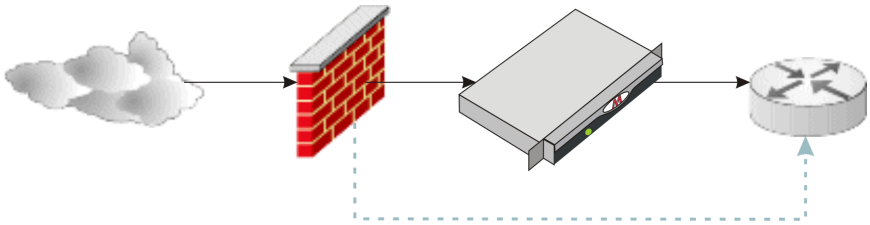


Abbildung 1-2 Platzierung im Modus "Transparente Bridge"

Platzieren Sie das Gerät im Modus "Transparente Bridge" zwischen der Firewall und Ihrem Router, wie in der Abbildung dargestellt.

In diesem Modus verbinden Sie zwei Netzwerksegmente physisch mit dem Gerät. Das Gerät behandelt diese als eine einzige logische Einheit. Da sich die Geräte – Firewall, Gerät und Router – im selben logischen Netzwerk befinden, müssen sie kompatible IP-Adressen im selben Subnetz haben.

Geräte auf der einen Seite der Bridge (z. B. ein Router), die mit den Geräten auf der anderen Seite der Bridge (z. B. einer Firewall) kommunizieren, bemerken die Bridge nicht. Sie erkennen nicht, dass der Datenverkehr abgefangen und gescannt wird. Deshalb wird dieser Betriebsmodus des Geräts als "Transparente Bridge" bezeichnet.

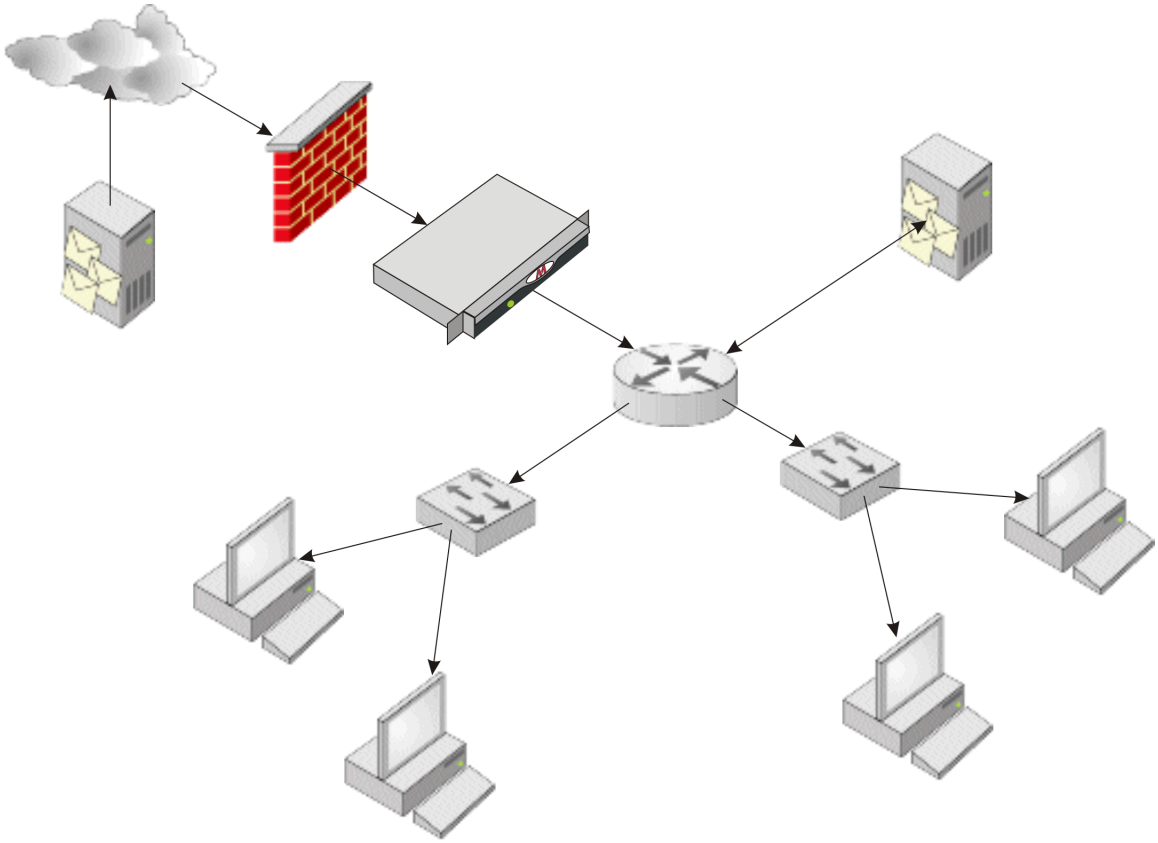


Abbildung 1-3 Netzwerkstruktur – Modus "Transparente Bridge"

Das Spanning Tree-Protokoll zum Verwalten der Bridge-Priorität

Konfigurieren Sie das Spanning Tree Protocol (STP), um die Bridge-Prioritäten für Ihren McAfee® Email Gateway Blade Server zu verwalten.

> **Bevor Sie beginnen**
>
> Der Blade-Server muss im Modus "Transparente Bridge" konfiguriert werden, damit das Spanning Tree-Protokoll zur Verfügung steht.

Sollte ein Blade ausfallen, leitet das Spanning Tree Protocol den Netzwerkverkehr direkt an das Blade mit der nächsthöheren Bridge-Priorität weiter.

Im Modus "Transparente Bridge" haben der Management-Blade-Server und der Failover-Management-Blade-Server unterschiedliche IP-Adressen.

In den Modi "Transparenter Router" und "Expliziter Proxy" haben die beiden Blades ebenfalls unterschiedliche IP-Adressen, werden jedoch mit derselben virtuellen IP-Adresse bzw. mit denselben virtuellen IP-Adressen konfiguriert.

Normalerweise wird der E-Mail-Verkehr vom Management-Blade-Server verarbeitet. Wenn dieses Blade ausfällt, wird der E-Mail-Verkehr vom Failover-Management-Blade-Server verarbeitet.

Jedes Blade hat eine andere Bridge-Priorität. Da der Management-Blade-Server höhere Priorität hat (beispielsweise den STP-Wert 100), verarbeitet normalerweise der Management-Blade-Server den Netzwerkverkehr bzw. fängt ihn ab.

Wenn der Management-Blade-Server ausfällt, leitet das STP den Netzwerkverkehr über einen Pfad mit der nächsthöheren Bridge-Priorität weiter, also an den Failover-Management-Blade-Server (beispielsweise mit einem STP-Wert von 200).

Vorgehensweise

1. Gehen Sie folgendermaßen vor, um Bridge-Loops zu vermeiden:
   a. Deaktivieren Sie STP auf den Anschlüssen 1 und 2 aller Interconnect-Module.
   b. Stellen Sie sicher, dass alle Anschlüsse Mitglieder der Spanning Tree Group 1 (STG1) sind.
   c. Deaktivieren Sie STG1.
2. Installieren Sie den Failover-Management-Blade-Server in Steckplatz 2.
3. Während der Einrichtung des Failover-Management-Blade-Servers stellen Sie für die Bridge-Priorität beispielsweise den Wert "200" ein.
4. Installieren Sie den Management-Blade-Server in Steckplatz 1.
5. Während der Einrichtung des Management-Blade-Servers stellen Sie für die Bridge-Priorität beispielsweise den Wert "100" ein.
6. Weisen Sie dem Management-Blade-Server und dem Failover-Management-Blade-Server unterschiedliche IP-Adressen zu.

Modus "Transparenter Router"

In diesem Abschnitt lernen Sie den Modus "Transparenter Router" des McAfee Email Gateways besser kennen.

Im Modus "Transparenter Router" scannt das Gerät den E-Mail-Verkehr zwischen zwei Netzwerken. Das Gerät hat eine IP-Adresse für ausgehenden gescannten Verkehr und muss eine IP-Adresse für eingehenden Verkehr haben.

Die kommunizierenden Netzwerkserver erkennen nicht, dass das Gerät zwischengeschaltet ist. Der Betrieb des Geräts ist für die Geräte transparent.

Arbeitsweise des Geräts im Modus "Transparente Router"

Im Modus "Transparenter Router" wird das Gerät mit den Netzwerken über den LAN1- und den LAN2-Anschluss verbunden. Das Gerät scannt den Datenverkehr, der über ein Netzwerk eingeht, und leitet ihn an das nächste Netzwerkgerät in einem anderen Netzwerk weiter. Das Gerät fungiert als Router (wobei es Datenverkehr zwischen den verschiedenen Netzwerken auf der Basis der Informationen in den Routing-Tabellen weiterleitet).

Konfiguration im Modus "Transparenter Router"

Im Modus "Transparenter Router" müssen Sie Ihre Netzwerkgeräte nicht explizit neu konfigurieren, damit der Datenverkehr an das Gerät gesendet wird. Sie müssen lediglich die Routing-Tabelle für das Gerät konfigurieren und einige der Routing-Informationen für die Netzwerkgeräte auf einer Seite des Geräts ändern (der Geräte also, die an die LAN1- und LAN2-Anschlüsse des Geräts angeschlossen sind). Es könnte zum Beispiel erforderlich sein, das Gerät als Standard-Gateway zu konfigurieren.

Im Modus "Transparenter Router" muss das Gerät zwei Netzwerke miteinander verbinden. Das Gerät muss innerhalb Ihres Unternehmens hinter einer Firewall platziert werden.

Im Modus "Transparenter Router" werden weder Multicast-IP-Datenverkehr noch andere Protokolle wie NETBEUI und IPX (Nicht-IP-Protokolle) unterstützt.

Firewall-Regeln

Im Modus "Transparenter Router" wird die Firewall mit der physischen IP-Adresse für die LAN1/LAN2-Verbindung mit dem Management-Blade-Server verbunden.

Platzieren des Geräts

Verwenden Sie das Gerät im Modus "Transparenter Router", um einen im Netzwerk vorhandenen Router zu ersetzen.

Wenn Sie den Modus "Transparenter Router" verwenden und keinen vorhandenen Router ersetzen, müssen Sie einen Teil Ihres Netzwerks neu konfigurieren, damit der Datenverkehr korrekt durch das Gerät fließt.

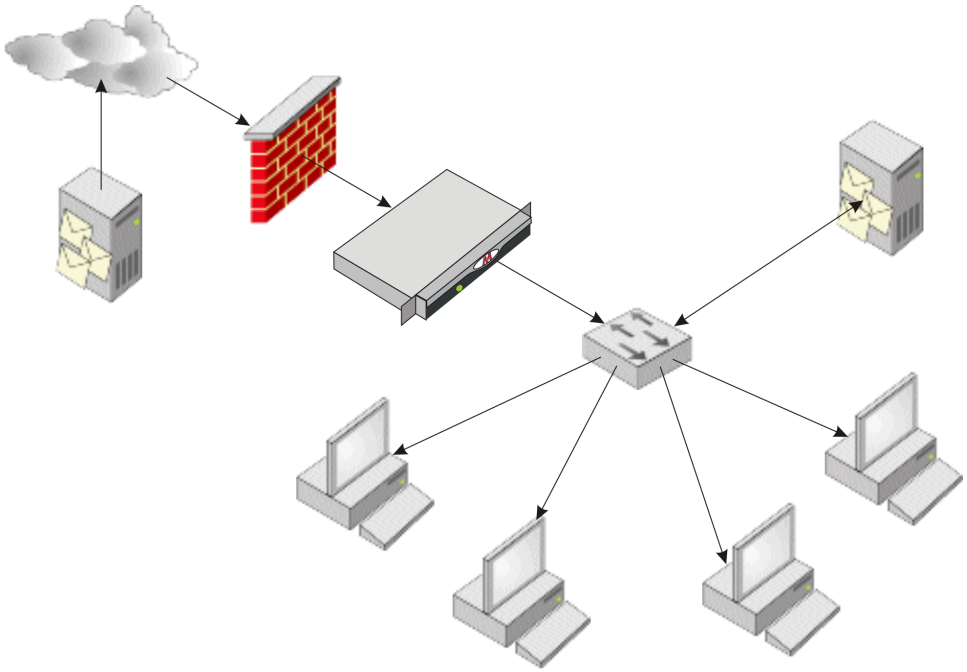


Abbildung 1-4 Netzwerkstruktur – Modus "Transparente Bridge"

Sie müssen wie folgt vorgehen:

- Konfigurieren Sie die Client-Geräte so, dass sie auf das Standard-Gateway verweisen.
- Konfigurieren Sie das Gerät so, dass das Internet-Gateway als Standard-Gateway verwendet wird.
- Stellen Sie sicher, dass Ihre Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.

Modus "Expliziter Proxy"

In diesem Abschnitt lernen Sie den Modus "Expliziter Proxy" des McAfee Email Gateways besser kennen.

Im Modus "Expliziter Proxy" müssen einige Netzwerkgeräte so eingerichtet werden, dass sie Datenverkehr explizit an das Gerät senden. Das Gerät fungiert dann als Proxy oder Relay und verarbeitet den Datenverkehr für die Geräte.

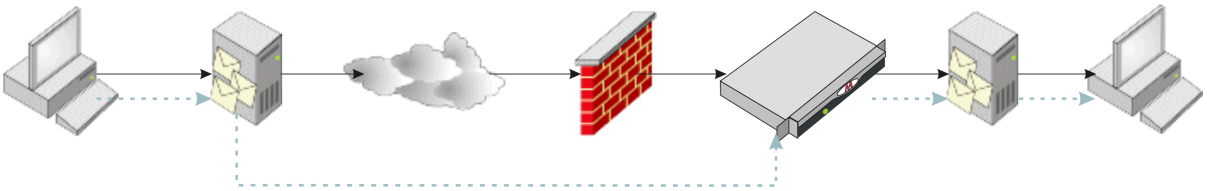


Abbildung 1-5 Modus "Expliziter Proxy" – sichtbarer Datenpfad

Der Modus "Expliziter Proxy" ist am besten für Netzwerke geeignet, in denen Client-Geräte über ein einzelnes Upstream- und Downstream-Gerät eine Verbindung zum Gerät herstellen.

Dies ist möglicherweise nicht die beste Option, wenn verschiedene Netzwerkgeräte erneut konfiguriert werden müssen, damit sie den Datenverkehr an das Gerät senden.

Netzwerk- und Gerätekonfiguration

Wenn sich das Gerät im Modus "Expliziter Proxy" befindet, müssen Sie den internen Mail-Server explizit so konfigurieren, dass er E-Mail-Verkehr an das Gerät sendet. Das Gerät prüft den E-Mail-Verkehr, bevor es ihn im Namen des Absenders an den externen Mail-Server weiterleitet. Der externe E-Mail-Server leitet die E-Mail dann an den Empfänger weiter.

Entsprechend muss das Netzwerk so konfiguriert werden, dass eingehende E-Mail-Nachrichten aus dem Internet nicht dem internen Mail-Server, sondern dem Gerät zugestellt werden.

Das Gerät kann den E-Mail-Verkehr dann prüfen, bevor es ihn im Namen des Absenders an den internen E-Mail-Server zur Zustellung weiterleitet, wie in der Abbildung dargestellt.

Beispielsweise kann ein externer Mail-Server direkt mit dem Gerät kommunizieren, auch wenn der Datenverkehr möglicherweise mehrere Netzwerkserver passiert, bevor er das Gerät erreicht. Der wahrgenommene Pfad verläuft vom externen Mail-Server zum Gerät.

Protokolle

Um ein unterstütztes Protokoll zu scannen, müssen Sie Ihre anderen Netzwerkserver oder Client-Computer so konfigurieren, dass das Protokoll durch das Gerät geleitet wird, sodass kein Datenverkehr das Gerät umgehen kann.

Firewall-Regeln

Im Modus "Expliziter Proxy" werden alle Firewall-Regeln, die für den Client-Zugriff auf das Internet eingerichtet wurden, außer Kraft gesetzt. Für die Firewall sind nur die physischen IP-Adressinformationen für das Gerät sichtbar, nicht jedoch die IP-Adressen der Clients. Die Firewall kann daher ihre Internetzugriffsregeln nicht auf die Clients anwenden.

Stellen Sie sicher, dass die Firewall-Regeln aktualisiert werden. Die Firewall muss den Datenverkehr vom McAfee® Email Gateway akzeptieren, darf aber keinen Datenverkehr verarbeiten, der direkt von den Client-Geräten kommt.

Richten Sie Firewall-Regeln ein, die verhindern, dass unerwünschter Datenverkehr in Ihr Unternehmen gelangt.

Platzieren des Geräts

Konfigurieren Sie die Netzwerkgeräte so, dass der zu scannende Datenverkehr an das McAfee® Email Gateway gesendet wird. Das ist wichtiger als der Standort des McAfee® Email Gateway.

Der Router muss allen Benutzern erlauben, eine Verbindung zum McAfee® Email Gateway herzustellen.

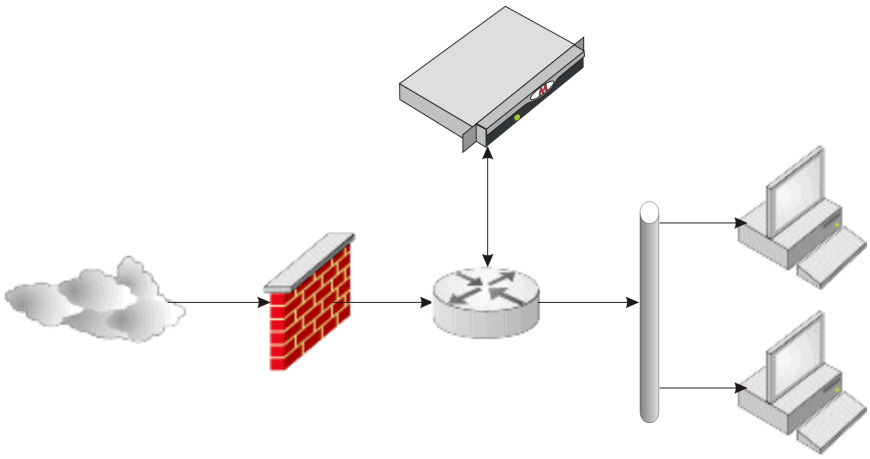


Abbildung 1-6 Platzierung im Modus "Expliziter Proxy"

Das McAfee® Email Gateway muss innerhalb Ihres Unternehmens hinter einer Firewall platziert werden, wie in Abbildung 6 dargestellt: Konfiguration als expliziter Proxy.

Normalerweise ist die Firewall so konfiguriert, dass der Datenverkehr, der nicht direkt von dem Gerät stammt, gesperrt wird. Wenn Sie in Bezug auf die Topologie Ihres Netzwerks unsicher sind und nicht wissen, wie Sie das Gerät integrieren sollen, wenden Sie sich an Ihren Netzwerkspezialisten.

Verwenden Sie diese Konfiguration in folgenden Fällen:

- Das Gerät wird im Modus "Expliziter Proxy" betrieben.
- Sie verwenden E-Mail (SMTP).

Für diese Konfiguration gilt:

- Konfigurieren Sie die externen DNS-Server (Domain Name System) oder NAT (Network Address Translation) auf der Firewall so, dass der externe Mail-Server E-Mails an das Gerät zustellt, nicht an den internen Mail-Server.
- Konfigurieren Sie die internen Mail-Server so, dass E-Mail-Verkehr an das Gerät gesendet wird. Das heißt, die internen Mail-Server müssen das Gerät als Smart-Host verwenden. Vergewissern Sie sich, dass die Client-Geräte E-Mails an die E-Mail-Server in Ihrem Unternehmen senden können.
- Stellen Sie sicher, dass die Firewall-Regeln aktualisiert werden. Die Firewall muss den Datenverkehr von dem Gerät akzeptieren, darf aber keinen Datenverkehr verarbeiten, der direkt von den Client-Geräten kommt. Richten Sie Regeln ein, die verhindern, dass unerwünschter Datenverkehr in Ihr Unternehmen gelangt.

Ausbringungsstrategien für die Verwendung des Geräts in einer DMZ

Lernen Sie demilitarisierte Zonen in Ihrem Netzwerk kennen, und erfahren Sie, wie Sie diese zum Schutz Ihrer E-Mail-Server verwenden können.

Eine "demilitarisierte Zone" (Demilitarized Zone, DMZ) ist ein Netzwerk, das durch eine Firewall von allen anderen Netzwerken getrennt ist, auch vom Internet und anderen internen Netzwerken. Eine DMZ wird üblicherweise mit dem Ziel implementiert, den Zugriff auf Server zu sperren, die Internetdienste (beispielsweise E-Mail) zur Verfügung stellen.

Hacker verschaffen sich oft Zugriff auf Netzwerke, indem sie herausfinden, auf welchen TCP-/UDP-Ports Appliances Anfragen erwarten, und dann bekannte Schwachstellen in Appliances ausnutzen. Firewalls senken das Risiko solcher Exploits erheblich, indem sie den Zugriff auf bestimmte Ports auf bestimmten Servern steuern.

Das Gerät kann einfach zu einer DMZ-Konfiguration hinzugefügt werden. Die Art, wie Sie das Gerät in einer DMZ verwenden, hängt von den zu scannenden Protokollen ab.

SMTP-Konfiguration in einer DMZ

Erfahren Sie, wie Sie SMTP-Geräte, die sich innerhalb einer demilitarisierten Zone Ihres Netzwerks befinden, konfigurieren.

Die DMZ ist eine gute Möglichkeit für das Verschlüsseln von E-Mails. Wenn der E-Mail-Verkehr die Firewall zum zweiten Mal erreicht (auf seinem Weg von der DMZ zum Internet), ist er verschlüsselt.

Geräte, die SMTP-Verkehr in einer DMZ scannen können, sind normalerweise im Modus "Expliziter Proxy" konfiguriert.

Konfigurationsänderungen müssen nur an den MX-Einträgen für die E-Mail-Server vorgenommen werden.

HINWEIS: Sie können den Modus "Transparente Bridge" verwenden, wenn Sie SMTP in einer DMZ scannen. Wenn Sie jedoch den Datenfluss nicht richtig steuern, scannt das Gerät jede Nachricht zweimal, einmal in jede Richtung. Aus diesem Grund wird für SMTP-Scans normalerweise der Modus "Expliziter Proxy" verwendet.

E-Mail-Relay

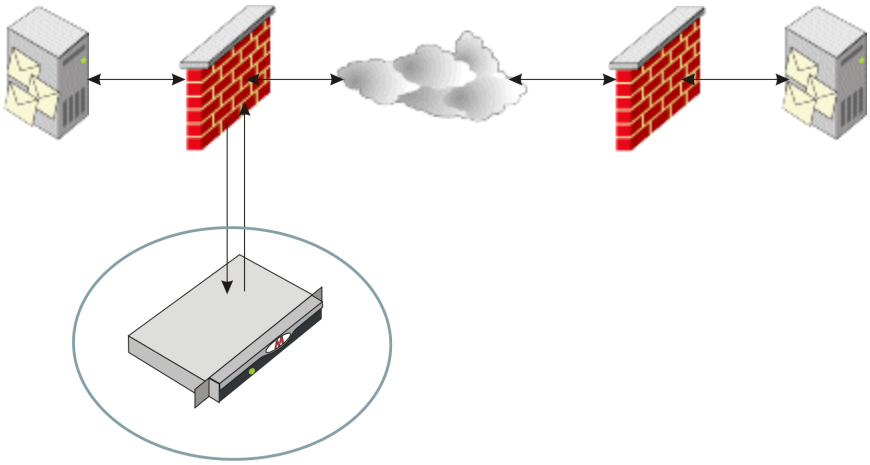


Abbildung 1-7 Konfigurieren als Mail-Relay

Wenn Sie in Ihrer DMZ bereits ein Relay eingerichtet haben, können Sie es durch das Gerät ersetzen.

Um Ihre bestehenden Firewall-Richtlinien zu verwenden, geben Sie dem Gerät dieselbe IP-Adresse wie dem Mail-Relay.

E-Mail-Gateway

SMTP bietet keine Methoden zur Verschlüsselung von E-Mail-Nachrichten. Sie können mithilfe von TLS (Transport Layer Security) den Link verschlüsseln, nicht jedoch die E-Mail-Nachrichten. Daher erlauben einige Unternehmen solchen Datenverkehr nicht in ihrem internen Netzwerk. Zur Umgehung dieses Problems wird häufig ein proprietäres E-Mail-Gateway eingesetzt, zum Beispiel Lotus Notes® oder Microsoft® Exchange, um den E-Mail-Datenverkehr zu verschlüsseln, bevor er das Internet erreicht.

Um eine DMZ-Konfiguration unter Verwendung des proprietären E-Mail-Gateways zu implementieren, fügen Sie das Scan-Gerät zur DMZ auf der SMTP-Seite des Gateways hinzu.

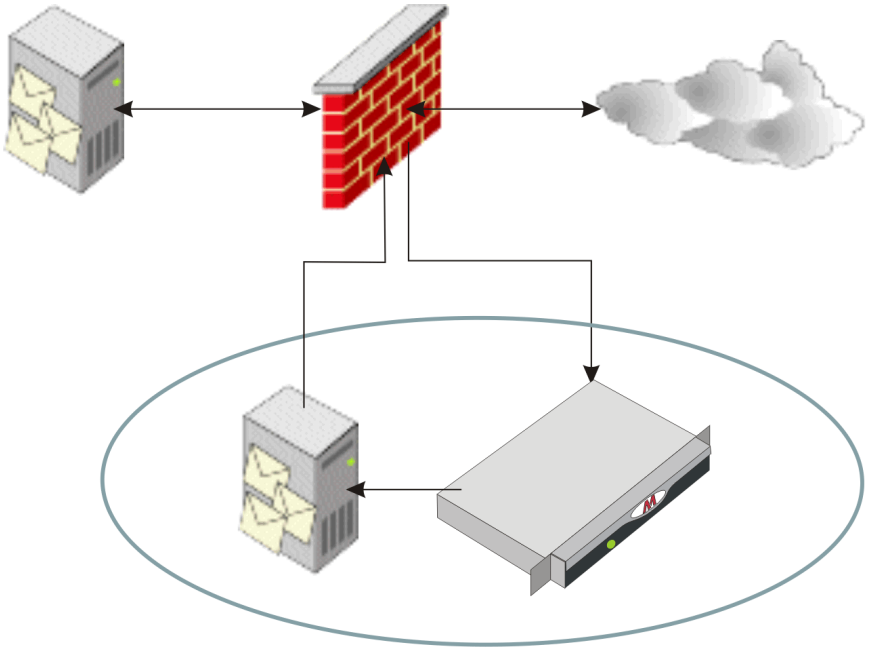


Abbildung 1-8 Konfigurieren als E-Mail-Gateway

Nehmen Sie hierfür folgende Konfigurationen vor:

- Die öffentlichen MX-Einträge müssen externe Mail-Server anweisen, alle eingehenden E-Mail-Nachrichten an das Gerät (statt an das Gateway) zu senden.
- Das Gerät muss alle eingehenden E-Mail-Nachrichten an das Mail-Gateway und alle ausgehenden Nachrichten per DNS oder über ein externes Relay senden.
- Das E-Mail-Gateway muss alle eingehenden E-Mails an die internen Mail-Server und aller andere (ausgehenden) Mails an das Gerät weiterleiten.
- Die Firewall erlaubt nur eingehende E-Mails, die sich an das Gerät richten.

Bei Firewalls, auf denen die Verwendung von NAT (Network Address Translation) konfiguriert ist und die eingehende E-Mails an die internen E-Mail-Server umleiten, müssen die öffentlichen MX-Einträge nicht neu konfiguriert werden. Sie leiten den Datenverkehr bereits an die Firewall und nicht an das eigentliche E-Mail-Gateway. In diesem Fall muss die Firewall neu konfiguriert werden, sodass eingehende Nachrichten an das Gerät geleitet werden.

Für Lotus Notes spezifische Firewall-Regeln

Erfahren Sie, welche speziellen Aspekte beim Schutz von Lotus Notes-Systemen zu berücksichtigen sind.

Lotus Notes-Server kommunizieren standardmäßig über TCP-Port 1352. Die für den Schutz von Notes-Servern in einer DMZ verwendeten Firewall-Regeln erlauben üblicherweise folgendem Datenverkehr das Passieren durch die Firewall:

- Eingehende SMTP-Anforderungen (TCP-Port 25) vom Internet, die für das Gerät bestimmt sind
- Anforderungen auf TCP-Port 1352 aus dem Notes-Gateway, die an einen internen Notes-Server gerichtet sind
- Anforderungen auf TCP-Port 1352 von einem internen Notes-Server, die an das Notes-Gateway gerichtet sind
- SMTP-Anforderungen vom Gerät, die für das Internet bestimmt sind

Alle anderen SMTP-Anforderungen und Anforderungen auf TCP-Port 1352 werden verweigert.

Für Microsoft Exchange spezifische Firewall-Regeln

Erfahren Sie, welche speziellen Aspekte beim Schutz von Microsoft Exchange-Systemen zu berücksichtigen sind.

Ein auf Microsoft Exchange basierendes E-Mail-System erfordert eine erhebliche Umkonfiguration.

Wenn Exchange-Server miteinander kommunizieren, senden sie die ersten Pakete mithilfe des RPC-Protokolls (TCP-Port 135). Sobald die ursprüngliche Kommunikation jedoch eingerichtet ist, werden zwei Ports dynamisch ausgewählt und verwendet, um alle nachfolgenden Pakete für den Rest der Kommunikation zu senden. Sie können die Firewall nicht so konfigurieren, dass sie diese dynamisch gewählten Ports erkennt. Deshalb leitet die Firewall diese Pakete nicht weiter.

Die Ausweichlösung lautet, die Registrierung auf jedem Exchange-Server zu modifizieren, der über die Firewall kommuniziert, sodass immer dieselben zwei "dynamischen" Ports verwendet werden, und dann TCP 135 und diese beiden Ports auf der Firewall zu öffnen.

Wir erwähnen diese Ausweichlösung, um eine umfassende Erklärung zu bieten, wir empfehlen sie jedoch nicht. Das RPC-Protokoll ist in Microsoft-Netzwerken weit verbreitet. Das Öffnen von TCP 135 für eingehenden Datenverkehr ist für die meisten Sicherheitsexperten ein rotes Tuch.

Wenn Sie diese Ausweichlösung verwenden möchten, finden Sie Details im folgenden KnowledgeBase-Artikel auf der Microsoft-Website:

http://support.microsoft.com/kb/q176466/

Arbeitslastverwaltung

In diesem Abschnitt lernen Sie Funktionen zur Arbeitslastverwaltung des McAfee Email Gateways kennen.

Die Appliance verfügt über eine eigene interne Arbeitslastverwaltung, durch die die Scan-Last gleichmäßig auf alle für die Zusammenarbeit konfigurierten Appliances verteilt wird.

Sie müssen kein separates externes Lastausgleichsystem bereitstellen.

2 Anschließen und Konfigurieren des Blade-Servers

In diesem Abschnitt lernen Sie die erforderlichen Konzepte, Vorgänge und Aspekte zum Anschließen und Konfigurieren Ihres Blade-Servers kennen.

Der McAfee Email Gateway Blade Server kann mit Ihrem Netzwerk verbunden und in den folgenden Modi konfiguriert werden:

- Standardmodus (nicht ausfallsicher)
- Ausfallsicherer Modus

Standardmodus (nicht ausfallsicher)

Im Standardmodus (nicht ausfallsicher) werden für die Verbindung Ihres Blade-Servers mit dem Netzwerk dieselben Komponenten und Prozesse verwendet, die bereits von vorherigen Versionen des McAfee Email Gateway Blade Server-Produkts genutzt wurden.

Im Standardmodus (nicht ausfallsicher) ist Ihr Blade-Server nicht gegen Hardwareausfälle geschützt. Um gegen Hardwareausfälle gewappnet zu sein, sollten Sie in Betracht ziehen, auf Ihrem Blade-Server, nachdem Sie diesen vollständig eingerichtet, konfiguriert und getestet haben, den ausfallsicheren Modus zu aktivieren.

Ausfallsicherer Modus

Nachdem Sie Ihren Blade-Server für den Standardmodus konfiguriert haben, lesen Sie das Thema "Betrieb im ausfallsicheren Modus", das detaillierte Informationen zum Wechsel in den ausfallsicheren Modus enthält.

McAfee Email Gateway Blade Server umfasst den Betrieb im ausfallsicheren Modus für den Blade-Server. In diesem Modus werden alle Verbindungen zwischen Ihrem Netzwerk und dem Blade-Server sowie die Verbindungen innerhalb des Blade-Server-Gehäuses so ausgelegt, dass mehrere Pfade verwendet werden können.

Auf diese Weise kann der Ausfall von Serverkomponenten, Netzwerkgeräten oder Verkabelung, die für Weiterleitung des Datenverkehrs zwischen Ihrem Netzwerk und dem Blade-Server verwendet werden, besser verkraftet werden.

Inhalt

- *Upgrades von früheren Versionen*
- *Standardinstallation*
- *Installieren der Software*
- *Verwenden der Konfigurationskonsole*

Upgrades von früheren Versionen

In diesem Abschnitt erfahren Sie, welche Upgrade-Optionen möglich sind.

In den folgenden Themen wird beschrieben, wie ein Upgrade eines vorhandenen McAfee Email Gateway Blade Server, auf dem Email and Web Security Appliance-Software ausgeführt wird, zur Verwendung der McAfee Email Gateway-Software durchgeführt wird.

Um ein Upgrade von Email and Web Security Version 5.6 auf McAfee Email Gateway durchführen zu können, müssen Sie zuerst eine Migration zum aktuellen Patch von McAfee Email Gateway Version 7.0 durchführen und anschließend von McAfee Email Gateway Version 7.0 zu McAfee Email Gateway migrieren.

Falls Sie den ausfallsicheren Modus verwenden möchten, müssen Sie die Interconnect-Module im Blade-Server physisch neu konfigurieren.

Für die Durchführung eines Upgrades von früheren Installationen auf McAfee Email Gateway müssen Sie Zeit für einen Netzwerkausfall vorsehen, da der Blade-Server während des Upgrades keinen Datenverkehr scannt.

Bevor Sie ein Upgrade der Software Ihres Management- und Failover-Management-Blade-Servers durchführen, lesen Sie *Konfigurieren der Interconnect-Module bei der Durchführung eines Upgrades von einer älteren Version* und – falls Sie den ausfallsicheren Modus verwenden möchten – *Nutzung der Hardware im ausfallsicheren Modus*.

Sie können McAfee Email Gateway nicht auf Ihrem bestehenden Blade-Server installieren und dabei alle zuvor konfigurierten Web-Protokolle beibehalten (weder Email and Web Security-Software mit aktiviertem Web-Scanner noch McAfee Web Gateway). Eine McAfee Email Gateway-Installation verarbeitet ausschließlich E-Mail.

Schritt	Beschreibung in diesem Thema
1. Sichern Sie die vorhandene Konfiguration.	Sichern der vorhandenen Konfiguration
2. Fahren Sie alle Scan-Blades herunter.	Herunterfahren der Scan-Blades
3. Fahren Sie beide Management-Blade-Server herunter.	Herunterfahren der Management-Blade-Server
4. Führen Sie ein Upgrade der Software auf beiden Management-Blade-Servern durch.	Upgrade der Software für den Management-Blade-Server
5. Installieren Sie die Scan-Blades neu.	Erneute Installation der Scan-Blades
6. Konfigurieren Sie den ausfallsicheren Modus (sofern erforderlich).	Entscheidung treffen zur Verwendung des ausfallsicheren Modus Aktivieren des ausfallsicheren Modus

Konfigurieren der Interconnect-Module bei der Aktualisierung von einer älteren Version

Erfahren Sie, wie die Interconnect-Module für den Standard- und den ausfallsicheren Modus konfiguriert werden müssen.

In McAfee Email Gateway Blade Server wurden einige Änderungen an der Art und Weise vorgenommen, wie der Blade-Server die Hardware, insbesondere die Interconnect-Module im Blade-Gehäuse, verwendet.

Frühere Versionen von McAfee Email Gateway Blade Server, auf denen die Email and Web Security-Appliance-Software ausgeführt wurde, verwendeten zwei Interconnect-Module, Interconnect-Modul 1 für LAN1 und Interconnect-Modul 2 für LAN2.

Die Hardware, die mit McAfee Email Gateway Blade Server geliefert wird, verwendet einen der folgenden Modi:

- Im Standardmodus (nicht ausfallsicher) Interconnect-Modul 1 für LAN1 und Interconnect-Modul 3 für LAN2
- Im ausfallsicheren Modus die Interconnect-Module 1 und 2 für LAN1 sowie die Interconnect-Module 3 und 4 für LAN2

Weitere Informationen hierzu finden Sie unter *Nutzung der Hardware im ausfallsicheren Modus*.

Sichern der vorhandenen Konfiguration

Gehen Sie wie nachfolgend beschrieben vor, um die vorhandene Konfiguration Ihres McAfee Email Gateway Blade Server zu sichern.

McAfee empfiehlt, eine vollständige Sicherung Ihrer Blade-Server-Konfiguration zu erstellen, bevor Sie eine Aktualisierung durchführen, auch dann, wenn Sie vorhaben, eine der Aktualisierungsoptionen zu verwenden, die eine Sicherung und Wiederherstellung Ihrer Konfiguration einschließen.

Vorgehensweise

1. Navigieren Sie in der Benutzeroberfläche zu **System** | **Systemverwaltung** | **Konfigurationsverwaltung**.
2. Wählen Sie die optionalen Elemente aus, die Sie in die Sicherung aufnehmen möchten (versionsabhängig). McAfee empfiehlt, vor der Aktualisierung Ihres Blade-Servers alle Optionen zu sichern.
3. Klicken Sie auf **Konfiguration sichern**.
4. Nach kurzer Zeit wird ein Dialogfeld angezeigt, in dem Sie die gesicherte Konfigurationsdatei auf Ihren lokalen Computer herunterladen können.

Herunterfahren der Scan-Blades

Gehen Sie wie nachfolgend beschrieben vor, um die Scan-Blades in Ihrem McAfee Email Gateway Blade Server herunterzufahren.

> **Bevor Sie beginnen**
>
> Stellen Sie sicher, dass Sie die Scan-Blades zu einem geeigneten Zeitpunkt herunterfahren, wenn der Netzwerkverkehr am geringsten ist und möglichst wenige Beeinträchtigungen entstehen.

Vorgehensweise

1. Navigieren Sie in der Benutzeroberfläche des Management-Blade-Servers zu **System** | **Systemverwaltung** | **Cluster-Verwaltung**.
2. Geben Sie das Administratorkennwort in das Textfeld ein.
3. Klicken Sie neben dem Scan-Blade, das Sie herunterfahren möchten, auf **Herunterfahren**.
4. Sofern erforderlich, wiederholen Sie den Vorgang für andere Scan-Blades, die Sie herunterfahren möchten.

Herunterfahren der Management-Blade-Server

Gehen Sie wie nachfolgend beschrieben vor, um den Management-Blade-Server oder den Failover-Management-Blade-Server in Ihrem McAfee Email Gateway Blade Server herunterzufahren.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die Management-Blade-Server zu einem geeigneten Zeitpunkt herunterfahren, wenn der Netzwerkverkehr am geringsten ist und möglichst wenige Beeinträchtigungen entstehen.

Prüfen Sie vor dem Herunterfahren des Management-Blade-Servers, ob das Herunterfahren aller Scan-Blades abgeschlossen ist.

Vorgehensweise

1. Navigieren Sie in der Benutzeroberfläche des Management-Blade-Servers oder Failover-Management-Blade-Servers, den Sie herunterfahren möchten, zu **System** | **Systemverwaltung** | **Cluster-Verwaltung**.
2. Geben Sie Ihr Kennwort in das Textfeld neben **Appliance beenden** ein.
3. Klicken Sie auf **Appliance beenden**.
4. Sofern erforderlich, wiederholen Sie den Vorgang für den verbleibenden Management-Blade-Server.

Upgrade der Software für den Management-Blade-Server

Gehen Sie wie nachfolgend beschrieben vor, um die Software zu aktualisieren, die auf den Management-Blade-Servern Ihres McAfee Email Gateway Blade Server installiert ist.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie mit dem integrierten Lights-Out-Modul von HP vertraut sind. Unter HP Integrated Lights-Out User Guide finden Sie weitere Informationen.

Gehen Sie wie nachfolgend beschrieben vor, um die McAfee Email Gateway Blade Server-Software zu aktualisieren, die auf dem Management-Blade-Server und dem Failover-Management-Blade-Server installiert ist.

Wenn Sie bei einem vorhandenen McAfee Email Gateway Blade Server ein Software-Upgrade auf die neueste Version durchführen, stellen Sie sicher, dass die Software nicht nur auf dem Management-Blade-Server, sondern auch auf dem Failover-Management-Blade-Server aktualisiert wird.

Sie können wählen, auf welche Weise die Blade-Server-Software aktualisiert werden soll:

- Vollständige Installation ausführen und dabei vorhandene Daten überschreiben
- Software unter Beibehaltung der Konfiguration und der E-Mail-Nachrichten installieren
- Software nur unter Beibehaltung der Netzwerkkonfiguration installieren
- Software nur unter Beibehaltung der Konfiguration installieren

Aufgrund einer Änderung der Architektur in der aktuellen Version der Software müssen Sie sicherstellen, dass bei der Verwendung einer Aktualisierungsmethode, die die Konfiguration der vorherigen Version übernimmt, die Cluster-Kennung einen Wert zwischen 0 und 255 erhält. Sie finden diese Einstellung unter **System** | **Systemverwaltung** | **Cluster-Verwaltung**.

Vorgehensweise

1 Fahren Sie den Management-Blade-Server, der aktualisiert werden soll, herunter.

2 Wählen Sie Ihre Installationsmethode:

- Legen Sie die CD-ROM mit der McAfee Email Gateway-Software in ein externes CD-ROM-Laufwerk ein, das an den zu aktualisierenden Management-Blade-Server angeschlossen ist.
- Stellen Sie eine Verbindung zu dem HP Onboard Administrator im Blade-Server-Gehäuse her, und greifen Sie anschließend mit dem integrierten Lights-Out-Modul von HP auf jedes einzelne Blade zu. Wählen Sie dazu **Enclosure Information** | **Device bay** (Gehäuseinformation, Komponenteneinschub).

Sie können die Software auch von einem am Blade oder am Gehäuse angeschlossenen USB-Laufwerk aus installieren.

3 Nachdem Sie sich beim HP Onboard Administrator angemeldet haben, wählen Sie über die integrierte Lights-Out-Konsole den gewünschten Management-Blade-Server aus.

Der Management-Blade-Server befindet sich in Steckplatz 1 und der Failover-Management-Blade-Server in Steckplatz 2 des Gehäuses.

4 Wählen Sie im HP Onboard Administrator **Gehäuseinformationen** | **Device bay** | **Boot-Optionen**.

5 Überprüfen Sie, ob **CD-ROM** in der Boot-Liste als erstes Gerät aufgeführt ist.

6 Wählen Sie die Registerkarte **Virtual Devices** (Virtuelle Geräte).

7 Klicken Sie auf **Momentary Press** (Kurz drücken), um den Management-Blade-Server von der CD-ROM zu starten.

8 Wählen Sie anhand der Eingabeaufforderungen die gewünschte Upgrade-Option und anschließend die zu installierenden Software-Images aus.

Erneute Installation der Scan-Blades

Führen Sie eine Neuinstallation der Scan-Blades innerhalb Ihres McAfee Email Gateway Blade Server durch.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie mit dem integrierten Lights-Out-Modul von HP vertraut sind. Weitere Informationen hierzu finden Sie im HP Integrated Lights-Out User Guide.

Vorgehensweise

1 Wählen Sie im HP Onboard Administrator **Gehäuseinformationen** | **Device bay**, um für den neu zu installierenden Scan-Blade eine Verbindung zur integrierten Lights-Out-Benutzeroberfläche von HP herzustellen.

2 Wählen Sie die Registerkarte **Boot Options** (Startoptionen).

3 Wählen Sie aus der Dropdown-Liste **One Time Boot from:** (Einmalig Starten von) die Option **PXE NIC ****.

4 Klicken Sie auf **Übernehmen**.

5 Wählen Sie die Registerkarte **Virtual Devices** (Virtuelle Geräte).

6 Klicken Sie auf **Momentary Press** (Kurz drücken), um das Scan-Blade von dem Image zu starten, das auf dem Management-Blade-Server gespeichert ist.

7 Wiederholen Sie diese Schritte für jedes Scan-Blade, das erneut installiert wird.

Standardinstallation

Installieren Sie McAfee Email Gateway Blade Server unter Verwendung der Standardinstallation.

Die folgende Tabelle enthält einen Überblick über die Installation Ihres McAfee Email Gateway Blade Server.

Die Tabelle enthält auch die ersten Schritte, wenn Sie Ihren Blade-Server im ausfallsicheren Modus installieren möchten.

Tabelle 2-1 Standardinstallationsschritte

Schritt	wird hier beschrieben.
1. Packen Sie alle Komponenten aus, und prüfen Sie den Inhalt anhand der Packlisten in der Kiste.	Packlisten
2. Montieren Sie das Gehäuse im Rack, und installieren Sie den Onboard Administrator (OA) und alle Interconnect-Module.	Montieren des Blade-Servers Installieren der Interconnect-Module **Siehe auch** HP BladeSystem c7000 Enclosure Quick Setup Instructions HP BladeSystem c7000 Enclosure Setup and Installation Guide HP Integrated Lights-Out User Guide
3. Schließen Sie die Peripheriegeräte und die Stromversorgung an.	Anschließen des Blade-Servers an das Stromnetz **Siehe auch** HP BladeSystem c7000 Enclosure Quick Setup Instructions HP BladeSystem c7000 Enclosure Setup and Installation Guide HP Integrated Lights-Out User Guide
4. Schließen Sie den Blade-Server an das Netzwerk an.	Verbindung mit dem Netzwerk
5. Konfigurieren Sie den HP Onboard Administrator.	HP BladeSystem c7000 Enclosure Setup and Installation Guide HP Integrated Lights-Out User Guide
6. Installieren Sie die Software auf den Management-Blade-Servern.	Installieren der Software
7. Führen Sie die grundlegende Konfiguration durch.	Verwenden der Konfigurationskonsole
8. Wählen Sie die zu installierende Software aus.	Software-Images
9. Installieren Sie die Blade-Server zum Scannen von Inhalten nacheinander, und führen Sie einen PXE-Start des Management-Blade-Servers aus.	Installieren der Software auf einem Blade-Server zum Scannen von Inhalten
10. Leiten Sie den Testnetzwerkverkehr durch den Blade-Server.	Testen der Konfiguration

Tabelle 2-1 Standardinstallationsschritte *(Fortsetzung)*

Schritt	wird hier beschrieben.
11. Testen Sie, ob der Netzwerkverkehr gescannt wird.	Testen der Konfiguration
12. Konfigurieren Sie Richtlinien und Berichte.	Verwenden von Richtlinien für die Verwaltung von Nachrichten-Scans
13. Konfigurieren Sie den Produktionsverkehr durch das System.	Verwenden der Konfigurationskonsole

Wenn Sie den Blade-Server an Ihr Netzwerk anschließen, können der E-Mail-Zugang oder andere Netzwerkdienste unterbrochen werden. Planen Sie einen Zeitraum ein, in dem das Netzwerk nicht verfügbar ist, vorzugsweise zu einer Zeit mit geringer Netzwerkauslastung.

Montieren des Blade-Servers

Der McAfee Email Gateway Blade Server muss am vorgesehenen Standort aufgestellt und installiert werden.

Weitere Informationen zur Demontage und Montage Ihrer Blade-Gehäuse und -Komponenten erhalten Sie unter HP BladeSystem c7000 Enclosure Quick Setup Instructions und HP BladeSystem c7000 Enclosure Setup and Installation Guide.

Vorgehensweise

1 Nehmen Sie den Blade-Server aus der Schutzverpackung, und legen Sie ihn auf eine ebene Fläche.

Aufgrund seines Gewichts sollten Sie den Blade-Server so nah wie möglich am vorgesehenen Installationsort auspacken.

2 Entfernen Sie die vorderen und hinteren Komponenten sowie den hinteren Käfig des Blade-Servers.

3 Montieren Sie den hinteren Käfig, die Netzteile, die Kühllüfter, die Interconnect-Module und die Onboard Administrator-Komponenten erneut.

McAfee empfiehlt, alle Stromversorgungen und Kühllüfter zu montieren und zu nutzen, um beim Ausfall einer Stromversorgungseinheit Redundanz zu gewährleisten.

4 Schließen Sie einen Monitor und eine Tastatur an den Blade-Server an.

5 Verbinden Sie die Netzkabel mit dem Monitor und dem Blade-Server, schließen Sie sie jedoch noch nicht an die Spannungsversorgung an.

Installieren der Interconnect-Module für den Standardmodus (nicht ausfallsicher)

Installieren Sie die Interconnect-Module im Gehäuse des McAfee Email Gateway Blade Server.

Bevor Sie Verbindungen aufbauen, müssen Sie die Ethernet-Interconnect-Module installieren und konfigurieren.

Tabelle 2-2 Schlüssel

#	Beschreibung
1	Anschlüsse für Stromversorgung
2	Interconnect-Modul 1 (verbindet mit LAN 1)

Tabelle 2-2 Schlüssel *(Fortsetzung)*

#	Beschreibung
3	Interconnect-Modul 3 (verbindet mit LAN 2) Wenn Sie auf bestehender Hardware ein Upgrade von früheren Versionen durchführen, lesen Sie *Konfigurieren der Interconnect-Module bei der Aktualisierung von einer älteren Version*.
4	Onboard-Administrator-Anschluss
5	Onboard-Administrator-Modul
6	Out-of-Band-Zugang (Anschluss 20) Dieser wird erst aktiviert, nachdem die Interconnect-Module konfiguriert wurden.

Die Interconnect-Module werden an der Rückseite des Gehäuses unter der oberen Kühllüfterreihe installiert.

Das Interconnect-Modul LAN 1 wird in das obere linke Interconnect-Modul-Fach eingesetzt, das Interconnect-Modul LAN 2 direkt darunter in das untere linke Interconnect-Modul-Fach.

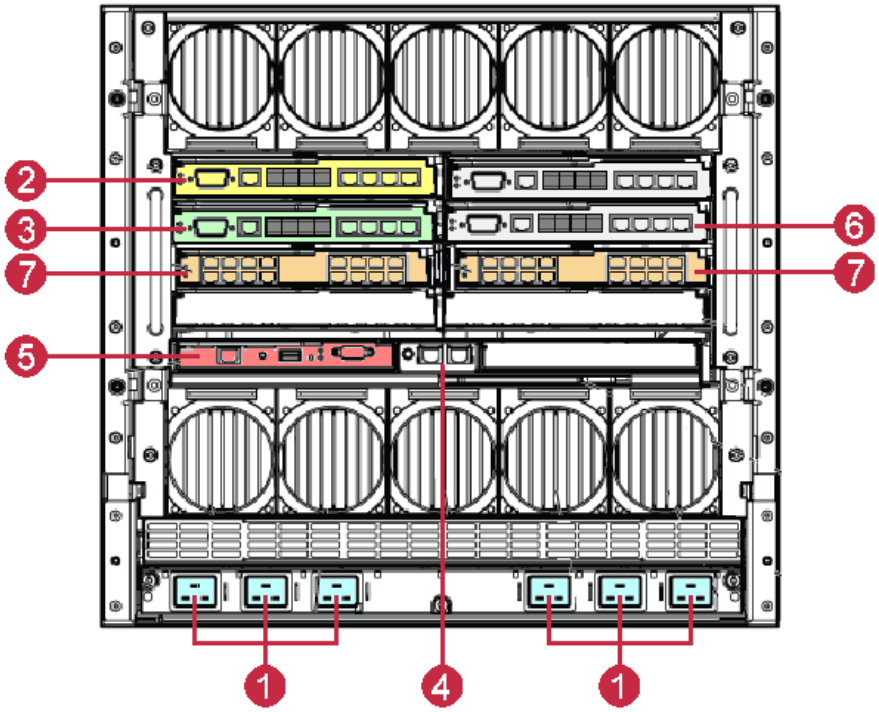


Abbildung 2-1 Positionen der Komponenten auf der Rückseite – Standardmodus (nicht ausfallsicher)

Führen Sie Folgendes aus:

- Deaktivieren Sie STP (Spanning Tree Protocol) für die STP-Gruppe 1 (standardmäßig sind alle Anschlüsse Mitglieder der STP-Gruppe 1). (Dies gilt, wenn Sie den Blade-Server im Modus "Transparente Bridge" installieren.)
- Konfigurieren Sie die ACLs (Access Control Lists, Zugriffssteuerungslisten) auf den Interconnect-Modulen so, dass die Blade-Server zum Scannen von Inhalten keine externen DHCP-Adressen empfangen können.

- Konfigurieren Sie die ACLs so, dass die Blade-Heartbeat-Pakete im Blade-Server verbleiben.
- Wenn für ein VLAN gekennzeichneter Datenverkehr durch den Blade-Server geleitet werden soll, müssen die Interconnect-Module so konfiguriert werden, dass sie diesen Datenverkehr durchlassen.

Informationen dazu, wie Sie dies tun, finden Sie in der unten aufgeführten Dokumentation:

- HP GbE2c Layer 2/3 Ethernet Blade Switch for c-Class BladeSystem Quick Setup
- HP GbE2c Layer 2/3 Ethernet Blade Switch for c-Class BladeSystem User Guide

Wenn Sie planen, den Blade-Server zu einem späteren Zeitpunkt für den Betrieb im ausfallsicheren Modus zu konfigurieren, sollten Sie in Erwägung ziehen, die erforderlichen Interconnect-Module bereits jetzt zu installieren. Anweisungen hierzu finden Sie unter *Installieren der Interconnect-Module für den ausfallsicheren Modus*.

Anschließen des Blade-Servers an das Stromnetz

Schließen Sie den McAfee Email Gateway Blade Server an die Stromversorgung an.

Um sicherzustellen, dass alle Blades mit Strom versorgt sind, verwenden Sie zwei unterschiedliche Stromkreise.

Wenn nur ein Stromkreis verwendet wird und die Einstellungen für die Stromversorgung für "Wechselstrom - redundant" konfiguriert sind (wie empfohlen), können einige Blades nicht hochgefahren werden.

Vorgehensweise

1 Schließen Sie die Netzkabel an die Blade-Netzteile und Stromsteckdosen an.

Falls die Netzkabel für das Einsatzland nicht geeignet sind, setzen Sie sich mit Ihrem Händler in Verbindung.

2 Schalten Sie den Blade-Server ein, indem Sie die Netzschalter am Management-Blade-Server und am Failover-Management-Blade-Server drücken.

Verwenden der Gleichstromnetzteile

Beachten Sie die Anforderungen für den Einsatz der Gleichstromnetzteile mit Ihrem McAfee Email Gateway Blade Server.

Wenn Sie die entsprechenden Netzteile erworben haben, kann der McAfee Email Gateway Blade Server an Gleichstromversorgungssysteme angeschlossen werden.

Informationen zur Verwendung von Gleichstromnetzteilen mit Ihrem McAfee Email Gateway Blade Server finden Sie im HP BladeSystem c7000 Carrier-Grade Enclosure Setup and Installation Guide.

Beachten Sie die folgenden Richtlinien bei der Installation des HP BladeSystem-Gleichstromnetzteils, um die Gefahr eines Stromschlags und Schäden an den Geräten zu vermeiden:

- Nur qualifizierte, im Umgang mit Gleichstromsystemen erfahrene Elektriker dürfen den McAfee Email Gateway Blade Server an Ihr Gleichstromversorgungssystem anschließen.
- Montieren Sie dieses Produkt nur an einem Standort mit eingeschränktem Zugang.
- Schließen Sie dieses Gerät an eine Gleichstromquelle an, die in Übereinstimmung mit den geltenden nationalen Vorschriften für Einrichtungen der Informationstechnik als Sekundärkreis klassifiziert werden kann.

  Im Allgemeinen basieren diese Anforderungen auf dem internationalen Standard für die Sicherheit von Einrichtungen der Informationstechnik, IEC 60950-1. Ein Pol (Neutral) der Stromquelle muss in Übereinstimmung mit den geltenden Vorschriften für die Stromversorgung geerdet sein.
- Schließen Sie dieses Gerät an einen Stromverteiler an, der die Möglichkeit bietet, den Stromkreis von der Stromversorgung zu trennen. Der Stromverteiler muss mit einem Überstromschutz ausgestattet sein, der Fehlerströme von der Hauptquelle unterbrechen kann und der für maximal 120 A ausgelegt ist.
- Verbinden Sie das grüngelbe Erdungskabel mit einem geeigneten Erdungsanschluss. Verlassen Sie sich nicht darauf, dass die Erdung über das Rack- oder Schrank-Chassis einen ausreichenden Durchgang gewährleistet.
- Stellen Sie sicher, dass die Geräte immer ordnungsgemäß geerdet sind und dass Sie bei der Erdung vorschriftsmäßig vorgegangen sind, bevor Sie mit einer Installation beginnen. Falsche Erdung kann zu elektrostatischer Entladung (ESD) und zu Schäden an elektronischen Bauteilen führen.

Verbindung mit dem Netzwerk

Erfahren Sie, wie Sie Ihr McAfee Email Gateway mit Ihrem Netzwerk verbinden.

Welche Interconnect-Module und Kabel Sie verwenden, um den Blade-Server an Ihr Netzwerk anzuschließen, hängt vom Netzwerkmodus ab, den Sie für den Blade-Server gewählt haben. Weitere Informationen über Netzwerkmodi finden Sie unter *Überlegungen zu Netzwerkmodi*.

Wenn Sie ein Upgrade von einer früheren Version mit einer vorhandenen Hardware durchführen, finden Sie unter *Konfigurieren der Interconnect-Module bei der Durchführung eines Upgrades von einer älteren Version* weitere Informationen darüber, welche Netzwerkverbindungen verwendet werden müssen.

Im Standardmodus sind die folgenden Verbindungen zwischen Ihrem Blade-Server und den Netzwerk-Switches erforderlich:

- **Modus "Transparente Bridge"** – Der Blade-Server fungiert als Bridge zwischen zwei Netzwerksegmenten. Schließen Sie das Interconnect-Modul 1 (LAN1) an ein Segment und das Interconnect-Modul 3 (LAN2) an das andere Segment an. Verwenden Sie dazu Kabel, die an einen der Anschlüsse 21 - 24 jedes Interconnect-Moduls angeschlossen sind. Die Verbindung zur Out-of-band-Verwaltung kann über einen anderen der LAN2-Anschlüsse hergestellt und konfiguriert werden.
- **Modus "Transparenter Router"** – Der Blade-Server fungiert als Router, der zwei separate Netzwerke miteinander verbindet. Schließen Sie das Interconnect-Modul 1 (LAN1) an ein Netzwerk und das Interconnect-Modul 3 (LAN2) an das andere Netzwerk an. Verwenden Sie dazu Kabel, die an einen der Anschlüsse 21 - 24 jedes Interconnect-Moduls angeschlossen sind. Die Verbindung zur Out-of-band-Verwaltung kann über einen anderen der LAN2-Anschlüsse hergestellt und konfiguriert werden.
- **Modus "Expliziter Proxy"** – Es wird eine einzelne Verbindung zwischen Interconnect-Modul 3 (LAN2) und Ihrem Netzwerk benötigt. (Bei Systemen, bei denen ein Upgrade durchgeführt wurde, wird LAN2 über das Interconnect-Modul 2 angeschlossen.) LAN1 kann für den Anschluss des Netzwerks verwendet werden, jedoch wird die maximale Leistung erreicht, wenn LAN1 für das Scanning-Netzwerk innerhalb des Blade-Servers verwendet wird. (Diese Einschränkung gilt nicht im ausfallsicheren Modus.)

Verwenden von Kupfer-LAN-Verbindungen

Erfahren Sie, wie Sie Ihr McAfee Email Gateway über Kupferkabel an Ihr Netzwerk anschließen.

Verwenden Sie die Interconnect-Module LAN1 und LAN2 sowie die im Lieferumfang enthaltenen Netzwerkkabel (oder entsprechende Cat-5e- bzw. Cat-6-Ethernet-Kabel), und schließen Sie den Blade-Server entsprechend dem gewählten Netzwerkmodus an Ihr Netzwerk an.

Modus "Transparente Bridge"

Schließen Sie die LAN1- und LAN2-Switches des E-Mail-Gateways mit den mitgelieferten Kupfer-LAN-Kabeln an Ihr Netzwerk an, um die Appliance in den Datenstrom einzufügen.

Modus "Transparenter Router"

Das E-Mail-Gateway fungiert als Router. Die LAN-Segmente, die mit den beiden Netzwerkschnittstellen verbunden sind, müssen sich deshalb in verschiedenen IP-Subnetzen befinden. Sie muss einen bestehenden Router ersetzen, oder auf der Seite der Appliance muss ein neues Subnetz angelegt werden. Ändern Sie hierfür die IP-Adresse oder die Netzmaske, die die Computer auf dieser Seite verwenden.

Modus "Expliziter Proxy"

Schließen Sie den LAN1- oder LAN2-Switch mit einem Kupfer-LAN-Kabel (mitgeliefert) an das Netzwerk an. Bei diesem Kabel handelt es sich um ein durchgängiges (ungekreuztes) Kabel, das die Appliance mit einem normalen, ungekreuzten RJ-45-Netzwerk-Switch verbindet.

LAN1 kann für den Anschluss des Netzwerks verwendet werden, jedoch wird die maximale Leistung erreicht, wenn LAN1 für das Scanning-Netzwerk innerhalb des Blade-Servers verwendet wird. (Diese Einschränkung gilt nicht im ausfallsicheren Modus.)

Verwenden von Glasfaser-LAN-Verbindungen

Erfahren Sie, wie Sie Ihr McAfee Email Gateway über Glasfaseroptikverbindungen an Ihr Netzwerk anschließen.

Bevor Sie Verbindungen herstellen, müssen Sie die Glasfaseroptik-SFP-Transceiver (Small Form-Factor Pluggable) installieren. Anweisungen dazu finden Sie unter HP GbE2c Layer 2/3 Ethernet Blade Switch for c-Class BladeSystem.

Verwenden Sie ausschließlich Glasfaseroptik-SFP-Transceiver von HP oder McAfee. Wenn Sie SFP-Transceiver anderer Hersteller verwenden, ist wahrscheinlich kein Zugriff auf den Blade-Server möglich.

Verwenden Sie die LAN1- und LAN2-Interconnect-Module und die Glasfaserkabel, und schließen Sie den Blade-Server entsprechend dem gewählten Netzwerkmodus an Ihr Netzwerk an.

Modus "Transparente Bridge"

Schließen Sie die Interconnect-Module LAN1 und LAN2 mit Glasfaserkabeln an das Netzwerk an.

Modus "Transparenter Router"

Schließen Sie die Interconnect-Module LAN1 und LAN2 mit Glasfaserkabeln an verschiedene IP-Subnetze an.

Modus "Expliziter Proxy"

Schließen Sie die LAN2-Interconnect-Module des Blade-Servers mit Glasfaserkabeln an das Netzwerk an.

LAN1 kann für den Anschluss des Netzwerks verwendet werden, jedoch wird die maximale Leistung erreicht, wenn LAN1 für das Scanning-Netzwerk innerhalb des Blade-Servers verwendet wird. (Diese Einschränkung gilt nicht im ausfallsicheren Modus.)

Installieren der Software

Die McAfee Email Gateway-Software muss sowohl auf dem Management-Blade-Server als auch auf dem Failover-Management-Blade-Server installiert werden.

Installationsreihenfolge der Management-Blade-Server

Installieren Sie beide Management-Blade-Server simultan.

Installieren Sie den Management-Blade-Server und den Failover-Management-Blade-Server in den Steckplätzen 1 und 2 des Blade-Server-Gehäuses.

Verbinden Sie beide Management-Blade-Server gemäß den Anweisungen unter *Installation der Software auf den Management-Blade-Servern*, und installieren Sie die Software.

Wenn Sie beide Management-Blade-Server gleichzeitig konfigurieren, sparen Sie nicht nur Zeit, sondern verhindern auch, dass dem zweiten Management-Blade-Server eine IP-Adresse im Scanning-Netzwerk zugewiesen wird, wenn der DHCP-Server des ersten Management-Blade-Servers gestartet wird.

Installation der Software auf den Management-Blade-Servern

Installieren Sie die Software auf dem Management-Blade-Server und auf dem Failover-Management-Blade-Server.

Bevor Sie beginnen

Sehen Sie nach, ob auf der McAfee-Download-Webseite neuere Versionen Ihrer Software erhältlich sind: http://www.mcafee.com/us/downloads/

Sie benötigen hierfür eine gültige Grant-Nummer.

Sie können die Software lokal auf dem Blade-Server installieren oder remote unter Verwendung der integrierten Lights-Out-Funktion. Die integrierte Lights-Out-Funktion stellt Einrichtungen für virtuelle Medien zur Verfügung, die Sie für das Remote-Mounten eines physischen CD-ROM-Laufwerks, einer ISO-Image-Datei oder eines USB-Laufwerks verwenden können, die die Installationsinformationen enthalten.

Vorgehensweise

1. Setzen Sie den Management-Blade-Server an Position 1 und den Failover-Management-Blade-Server an Position 2 des Blade-Server-Gehäuses ein.
2. Schließen Sie Folgendes an den Blade-Server an:
   - Schließen Sie über das mitgelieferte Kabel einen Monitor, eine Tastatur und ein USB-CD-ROM-Laufwerk an den weiterleitenden Konnektor des Management-Blade-Servers oder des Failover-Management-Blade-Servers an.
   - Bei einer Remote-Installation greifen Sie auf die integrierten Lights-Out-Module zu, indem Sie über den Onboard Administrator eine Remote-KVM-Sitzung aufbauen.
3. Starten Sie den Management-Blade-Server oder den Failover-Management-Blade-Server von der Installations- und Wiederherstellungs-CD. Die Software wird auf dem ausgewählten Blade installiert.
4. Legen Sie die grundlegende Konfiguration fest. Nähere Informationen hierzu finden Sie unter *Verwenden der Konfigurationskonsole*.

Synchronisierung von Konfigurationsänderungen

Erfahren Sie, wie Konfigurationsänderungen zwischen den Blades synchronisiert werden.

Alle Änderungen, die Sie auf dem Management-Blade-Server an der Konfiguration vornehmen, werden automatisch mit dem Failover-Management-Blade-Server und den Blade-Servern zum Scannen von Inhalten synchronisiert.

Überprüfen Sie auf dem **Dashboard** den Status des Management- und des Failover-Management-Blade-Servers, um sicherzustellen, dass die Synchronisierung stattgefunden hat.

Installieren der Software auf einem Blade-Server zum Scannen von Inhalten

Installieren Sie die Software auf einem Blade-Server zum Scannen von Inhalten.

Vorgehensweise

1 Wählen Sie in der Benutzeroberfläche die Option **Dashboard**. Unten auf der Seite wird **Blade-Status** angezeigt.

2 Setzen Sie den Blade-Server zum Scannen von Inhalten in das Gehäuse ein. Das Blade wird auf der Seite **Blade-Status** mit dem Status **INSTALLIEREN** angezeigt. Die Software wird vom Management-Blade-Server automatisch auf dem Blade-Server zum Scannen von Inhalten installiert. Dieser Vorgang dauert etwa 10 Minuten.

3 Die Daten werden automatisch aktualisiert. Nach einigen Minuten ändert sich der Status in **BOOT**, anschließend in **SYNC** und dann in **OK**.

Der neue Blade-Server zum Scannen von Inhalten ist nun funktionsbereit.

Verwenden der Konfigurationskonsole

Erfahren Sie, wie Sie das McAfee Email Gateway mithilfe der Konfigurationskonsole einrichten.

Sie können Ihr McAfee Email Gateway Blade Server entweder von der Konfigurationskonsole aus oder innerhalb der Benutzeroberfläche mit dem Setup-Assistenten konfigurieren.

Die Konfiguration wird nur auf die Management-Blade-Server und die Failover-Management-Blade-Server übernommen, nicht jedoch auf die Scan-Blades.

Die Konfigurationskonsole wird am Ende der Startsequenz automatisch gestartet, entweder nachdem:

- ein nicht konfiguriertes McAfee Email Gateway gestartet wurde,
- oder nachdem ein McAfee Email Gateway auf die Werkseinstellungen zurückgesetzt wurde.

Nach dem Start bietet Ihnen die **Konfigurationskonsole** Optionen, um Ihr Gerät von der McAfee Email Gateway-Konsole aus in Ihrer bevorzugten Sprache zu konfigurieren, bzw. liefert Anweisungen dafür, wie Sie von einem anderen Computer im selben Klasse-C-Subnetz (/24) aus eine Verbindung mit dem **Setup-Assistenten** innerhalb der Benutzeroberfläche herstellen können. Beide Methoden bieten Ihnen dieselben Optionen für die Konfiguration Ihres McAfee Email Gateway.

Von der **Konfigurationskonsole** aus können Sie eine neue Installation der Appliance-Software konfigurieren. Wenn Sie jedoch für die Konfiguration Ihrer Appliance eine zuvor gespeicherte Konfigurationsdatei verwenden möchten, müssen Sie sich bei der Benutzeroberfläche der Appliance anmelden und den Setup-Assistenten ausführen (**System | Setup-Assistent**).

Ebenso wird mit dieser Softwareversion für folgende Parameter die automatische Konfiguration mithilfe von DHCP eingeführt:

- Host-Name
- Domänenname
- Standard-Gateway
- DNS-Server
- Geleaste IP-Adresse
- NTP-Server

Weitere Informationen zu jeder Seite der **Konfigurationskonsole** und des **Setup-Assistenten** erhalten Sie auf dem Bildschirm.

Durchführen der benutzerdefinierten Einrichtung

In diesem Abschnitt erfahren Sie, welchen Zweck die benutzerdefinierte Einrichtung hat.
Die **Benutzerdefinierte Einrichtung** ermöglicht Ihnen eine größere Kontrolle über die Optionen, die Sie auswählen können, darunter den Betriebsmodus des Geräts. Sie können auswählen, dass der E-Mail-Verkehr über die Protokolle SMTP und POP3 geschützt wird. Verwenden Sie diese Konfigurationsoption, um IPv6 zu konfigurieren und sonstige Änderungen an der Standardkonfiguration vorzunehmen.

Bei der **Benutzerdefinierten Einrichtung** enthält der Assistent die folgenden Seiten:

- **E-Mail-Konfiguration**
- **Grundlegende Einstellungen**
- **Netzwerkeinstellungen**
- **Cluster-Verwaltung**
- **DNS und Routing**
- **Zeiteinstellungen**
- **Kennwort**
- **Zusammenfassung**

Wiederherstellung aus einer Datei

In diesem Abschnitt erfahren Sie, welchen Zweck die Wiederherstellung aus einer Datei hat.
Wenn Sie Ihr Gerät über den **Setup-Assistenten** innerhalb der Benutzeroberfläche konfigurieren, können Sie mithilfe der Option **Aus Datei wiederherstellen** zuvor gespeicherte Konfigurationsdaten importieren und auf Ihr Gerät übernehmen. Nachdem diese Daten importiert wurden, können Sie Änderungen vornehmen, bevor Sie die Konfiguration anwenden.

Die Option **Aus Datei wiederherstellen** ist in der **Konfigurationskonsole** nicht verfügbar. Zum Verwenden dieser Option müssen Sie sich beim McAfee Email Gateway anmelden und **Aus Datei wiederherstellen** aus dem Menü **System** | **Setup-Assistent** auswählen.

Nachdem die Konfigurationsdaten importiert wurden, werden die Optionen der **Benutzerdefinierten Einrichtung** im **Setup-Assistenten** angezeigt (siehe *Durchführen der benutzerdefinierten Einrichtung*). Alle importierten Optionen werden auf den Assistentenseiten angezeigt, sodass Sie die Möglichkeit zum Vornehmen von Änderungen haben, bevor Sie die Konfiguration übernehmen.

Bei Verwendung der Option **Aus Datei wiederherstellen** enthält der Assistent die folgenden Seiten:

- **Konfigurationsdatei importieren**
- **Wiederherzustellende Werte**

Nachdem diese Informationen geladen wurden, werden die Seiten der **Benutzerdefinierten Einrichtung** angezeigt, in denen Sie weitere Änderungen vornehmen können, bevor Sie die neue Konfiguration übernehmen:

- **E-Mail-Konfiguration**
- **Grundlegende Einstellungen**
- **Netzwerkeinstellungen**
- **Cluster-Verwaltung**
- **DNS und Routing**
- **Zeiteinstellungen**
- **Kennwort**
- **Zusammenfassung**

Setup im Modus 'Nur Verschlüsselung'

In diesem Abschnitt erfahren Sie, welchen Zweck die Einrichtungsoptionen im Modus "Nur Verschlüsselung" haben.
In kleinen bis mittleren Organisationen ist es häufig ausreichend, dasselbe McAfee Email Gateway für E-Mail-Scan- und E-Mail-Verschlüsselungs-Tasks zu verwenden.

Wenn Sie jedoch in einem größeren Unternehmen bzw. in einer Branche arbeiten, in der die Zustellung des gesamten oder eines überwiegenden Teils des E-Mail-Aufkommens auf eine sichere Weise erfolgen muss, kann es empfehlenswert sein, eine oder mehrere McAfee Email Gateway Appliances als eigenständige Verschlüsselungs-Server einzurichten.

Unter diesen Umständen bieten Ihnen die Optionen für das **Setup im Modus "Nur Verschlüsselung"** innerhalb des **Setup-Assistenten** die relevanten Einstellungen, die für den Betrieb im Modus "Nur Verschlüsselung" erforderlich sind.

3 Vorstellung des Dashboards

In diesem Abschnitt wird die Seite **Dashboard** beschrieben und erläutert, wie ihre Voreinstellungen bearbeitet werden.

Inhalt

- *Das Dashboard*
- *Funktionen des Blade-Servers*

Das Dashboard

Das **Dashboard** bietet eine Zusammenfassung der Aktivitäten der Appliance.

Dashboard

Von dieser Seite aus können Sie auf die meisten Seiten zugreifen, die die Appliance steuern.

Auf einem Master-Blade von McAfee Email Gateway Blade Server können Sie diese Seite zudem verwenden, um eine Zusammenfassung aller Aktivitäten auf den Scan-Blades im McAfee Email Gateway Blade Server anzuzeigen.

Vorteile der Verwendung des Dashboards

Das **Dashboard** bietet einen zentralen Ort, an dem Sie Zusammenfassungen der Appliance-Aktivitäten mithilfe verschiedener Portlets ansehen können.

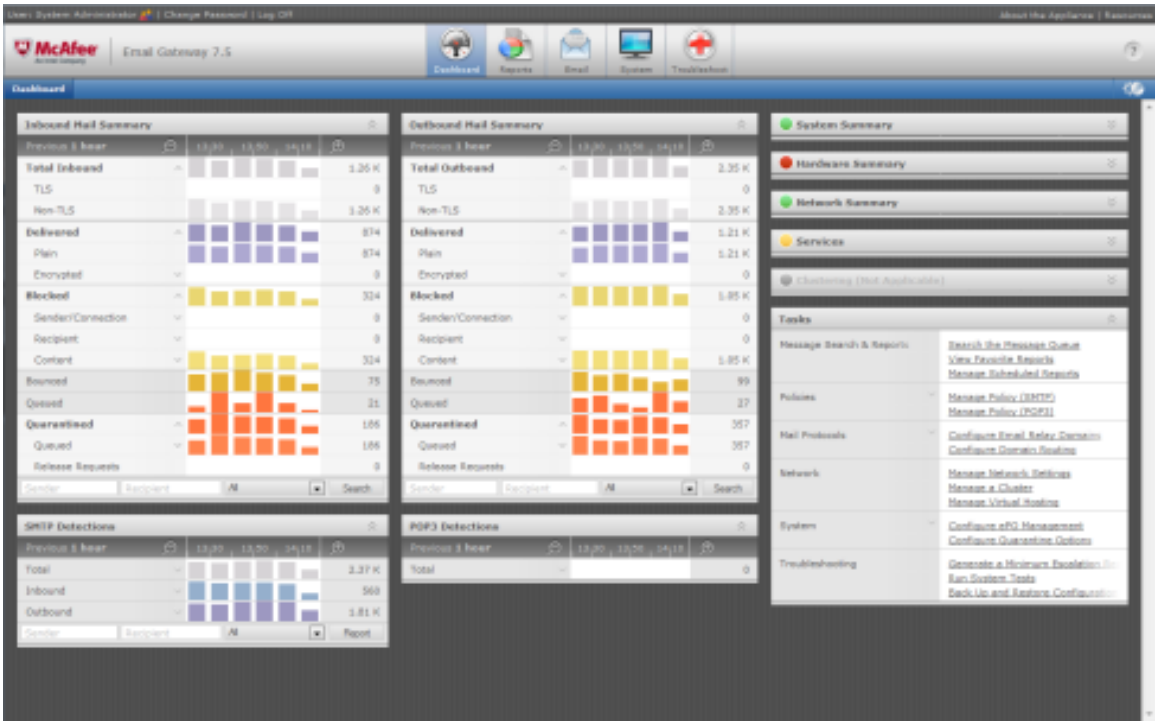


Abbildung 3-1 Dashboard-Portlets

In einigen Portlets werden Grafiken angezeigt, die die Appliance-Aktivität in den folgenden Zeiträumen darstellen:

- 1 Stunde
- 1 Tag (Standard)
- 1 Woche
- 2 Wochen
- 4 Wochen

Im **Dashboard** können Sie einige Änderungen an den angezeigten Informationen und Diagrammen vornehmen:

- Vergrößern und verkleinern Sie die Portlet-Daten mithilfe der Schaltflächen und rechts oben im Portlet.
- Zeigen Sie mithilfe der Schaltflächen und detailliertere Daten an.
- Eine Statusanzeige gibt an, ob das Element Aufmerksamkeit erfordert:
  - **Fehlerfrei**: Die ausgewiesenen Elemente funktionieren normal.
  - **Erfordert Aufmerksamkeit**: Ein Warnungsschwellenwert wurde überschritten.
  - **Erfordert sofortige Aufmerksamkeit**: Ein kritischer Schwellenwert wurde überschritten.
  - **Deaktiviert**: Der Dienst ist nicht aktiviert.

- Verwenden Sie und , um auf einer Zeitachse in Informationen herein- und herauszuzoomen. Es kommt zu einer kurzen Verzögerung, während die Ansicht aktualisiert wird. Standardmäßig zeigt das **Dashboard** Daten für den vorherigen Tag an.
- Verschieben Sie ein Portlet an eine andere Stelle auf dem **Dashboard**.
- Doppelklicken Sie auf die obere Leiste eines Portlets, um es auf den oberen Bereich des **Dashboards** zu vergrößern.
- Legen Sie eigene Warnhinweis- und Warnungsschwellenwerte zum Auslösen von Ereignissen fest. Markieren Sie dazu das Element, und klicken Sie darauf, bearbeiten Sie die Felder "Warnhinweisschwellenwert" und "Warnungsschwellenwert", und klicken Sie auf **Speichern**. Wenn das Element den von Ihnen festgelegten Schwellenwert überschreitet, wird ein Ereignis ausgelöst.

Abhängig von dem Browser, der zum Anzeigen der Benutzeroberfläche von McAfee Email Gateway verwendet wird, speichert das **Dashboard** den aktuellen Status jedes Portlets (ob es vergrößert oder verkleinert ist und ob Sie die Anzeige bestimmter Daten geöffnet haben) und versucht, die entsprechende Ansicht wiederherzustellen, wenn Sie zu einer anderen Seite in der Benutzeroberfläche navigieren und anschließend innerhalb derselben Browsersitzung zum **Dashboard** zurückkehren.

Dashboard-Portlets

Lernen Sie die Portlets auf dem Dashboard der Benutzeroberfläche von McAfee Email Gateway kennen.

Option	Beschreibung
Zusammenfassung der eingehenden E-Mails	Mit dem Portlet **Zusammenfassung der eingehenden E-Mails** können Sie Zustell- und Statusinformationen über Nachrichten abrufen, die an Ihr Unternehmen gesendet wurden.
Zusammenfassung der ausgehenden E-Mails	Mit dem Portlet **Zusammenfassung der ausgehenden E-Mails** können Sie Zustell- und Statusinformationen über Nachrichten abrufen, die von Ihrem Unternehmen aus gesendet wurden.
SMTP-Entdeckungen	Mit dem Portlet **SMTP-Entdeckungen** können Sie die Gesamtanzahl der Nachrichten feststellen, die eine Entdeckung basierend auf Absender, Verbindung, Empfänger oder Inhalt ausgelöst haben, bzw. Daten zum eingehenden oder ausgehenden SMTP-Datenverkehr anzeigen.
POP3-Entdeckungen	Mit dem Portlet **POP3-Entdeckungen** können Sie anzeigen, wie viele Nachrichten eine Entdeckung basierend auf Bedrohungen wie Viren, Komprimierungsprogrammen oder potenziell anstößigen Bildern ausgelöst haben.
Systemzusammenfassung	Mit dem Portlet **Systemzusammenfassung** können Sie Informationen über den Lastausgleich, den für jede Partition verwendeten Speicherplatz, die gesamte CPU-Auslastung, den verwendeten und verfügbaren Arbeitsspeicher sowie Swap-Details anzeigen.
Hardware-Zusammenfassung	Das Portlet **Hardware-Zusammenfassung** verwendet Statusindikatoren, um den Status von Netzwerkschnittstellen, USV-Servern, des Bridge-Modus (sofern aktiviert) sowie den RAID-Status anzuzeigen.
Netzwerkzusammenfassung	Mit dem Portlet **Netzwerkzusammenfassung** können Sie Informationen über den Status Ihrer Verbindungen, den Netzwerkdurchsatz und Zähler in Bezug auf die Kernel-Modus-Blockierung anzeigen.
Dienste	Mit dem Portlet **Dienste** können Sie Statistiken zum Aktualisierungs- und Dienststatus anzeigen, die auf den von der Appliance verwendeten Protokoll- und externen Servern basieren.

Option	Beschreibung
Clustering	Mit dem Portlet **Clustering** können Sie nach der Konfiguration Ihrer Appliance als Bestandteil eines Clusters oder bei Verwendung der Blade-Server-Hardware Informationen über den gesamten Cluster bereitstellen.
Tasks	Mit dem Portlet **Tasks** gelangen Sie direkt zu den Bereichen der Benutzeroberfläche, in denen Sie die Nachrichtenwarteschlange durchsuchen, Berichte anzeigen, Richtlinien verwalten, E-Mail-Protokoll-, Netzwerk- und System-Einstellungen konfigurieren und auf Funktionen zur Fehlerbehebung zugreifen können.

Vorgehensweise – Deaktivieren des Warnhinweises *McAfee Global Threat Intelligence-Feedback deaktiviert*

Hier wird beschrieben, wie Sie den Warnhinweis deaktivieren, dass McAfee Global Threat Intelligence-Feedback derzeit auf Ihrer Appliance deaktiviert ist.

Die Appliance zeigt standardmäßig eine Warnmeldung an, wenn das McAfee Global Threat Intelligence-Feedback (GTI-Feedback) nicht aktiviert ist, da es von McAfee als bewährte Vorgehensweise angesehen wird, diese Form der Kommunikation zu aktivieren.

Wenn Sie jedoch in einer Umgebung arbeiten, in der GTI-Feedback nicht aktiviert werden kann, gehen Sie wie nachfolgend beschrieben vor, um den Warnhinweis zu deaktivieren.

Vorgehensweise

1 Wählen Sie im Appliance-Dashboard im Bereich "Systemstatus" die Option **Bearbeiten** aus.

2 Deaktivieren Sie **Einen Warnhinweis anzeigen, wenn McAfee GTI-Feedback nicht aktiviert ist.**

3 Klicken Sie auf **OK**.

Der Warnhinweis *McAfee Global Threat Intelligence-Feedback deaktiviert* ist jetzt nicht mehr ausgewählt.

Funktionen des Blade-Servers

Lernen Sie anhand der Vorgehensweisen und Szenarien die wesentlichen Vorteile beim Einsatz eines Blade-Servers zum Schutz Ihres E-Mail-Verkehrs kennen.

Zur Durchführung dieser Vorgehensweisen und Szenarien benötigen Sie einige der Informationen, die Sie in der Konfigurationskonsole und im Setup-Assistenten eingegeben haben.

Demonstrieren der Failover- und Arbeitslastverwaltung

Demonstrieren Sie die Arbeitslastverwaltung und die integrierte Redundanzverwaltung des Blade-Servers.

Mit dem Blade-Server wird mindestens ein Blade-Server zum Scannen von Inhalten ausgeliefert. Sie können später weitere hinzufügen, falls erforderlich. Für diesen Test wird vorausgesetzt, dass zwei Blades zum Scannen von Inhalten vorhanden sind.

Informationen zum Hinzufügen und Entfernen von Blades aus dem Gehäuse finden Sie unter HP BladeSystem c3000 Enclosure Quick Setup Instructions oder HP BladeSystem c7000 Enclosure Quick Setup Instructions.

Vorgehensweise

1 Wählen Sie auf der Seite "Dashboard | Blade" die Registerkarte "Blade-Status" aus, um sicherzustellen, dass der Blade-Server ordnungsgemäß funktioniert.

- Der Management-Blade-Server hat den Namen, den Sie mithilfe der Konfigurationskonsole angegeben haben. Der Management-Blade-Server hat den Status **NETZWERK**.
- Der Failover-Management-Blade-Server hat den Namen, den Sie mithilfe der Konfigurationskonsole angegeben haben. Der Failover-Management-Blade-Server hat den Status **REDUNDANT**.
- Die Blade-Server zum Scannen von Inhalten werden mit "Blade01", "Blade02" usw. bezeichnet und haben den Status **OK**.

2 Fahren Sie den Management-Blade-Server herunter, nehmen Sie ihn aus dem Gehäuse, und beobachten Sie, wie der Blade-Server unter Einsatz des Failover-Management-Blade-Servers weiterhin funktioniert.

- Der Status des Failover-Management-Blade-Servers ändert sich in **Netzwerk**.
- Der Status des Management-Blade-Servers ändert sich in **Fehlgeschlagen**.

3 Wählen Sie unter **System | Cluster-Verwaltung** einen Blade-Server zum Scannen von Inhalten aus, und klicken Sie auf **Deaktivieren**, um diesen Blade-Server zum Scannen von Inhalten zu deaktivieren. Der Blade-Server setzt das Scannen des Datenverkehrs fort.

Das Design des Blade-Servers erlaubt die Entfernung eines Blade-Servers zum Scannen von Inhalten aus dem Gehäuse, ohne dass dieser zuerst gestoppt werden muss. McAfee empfiehlt dies jedoch nicht, da ein geringes Risiko besteht, dass dadurch die Informationen auf den Festplattenlaufwerken beschädigt werden könnten.

4 Sehen Sie sich die Spalte **Nachrichten** an, um die Anzahl der Nachrichten zu sehen, die von jedem Blade-Server zum Scannen von Inhalten verarbeitet werden.

5 Wählen Sie unter **Blade-Status** den Blade-Server zum Scannen von Inhalten aus, den Sie deaktiviert haben, und klicken Sie auf "Start".

6 Sehen Sie sich die Spalte "Nachrichten" erneut an. Der Blade-Server scannt weiteren Datenverkehr und gleicht automatisch die Scan-Last zwischen den beiden Blades aus.

7 *Optional*: Fügen Sie einen dritten Blade-Server zum Scannen von Inhalten zum Gehäuse hinzu, und aktivieren Sie ihn.

8 Sehen Sie sich erneut den **Blade-Status** an. Der Blade-Server scannt noch mehr Nachrichten und gleicht die Scan-Last zwischen den drei Blades aus.

Testen der Verwaltungsfunktionen auf dem Blade-Server

Demonstrieren Sie, wie die Verwaltungsfunktionen des Blade-Servers Ihren Systemverwaltungsaufwand senken. Das System wird wie ein einziges System verwaltet, unabhängig davon, ob Sie einen oder mehrere Blade-Server zum Scannen von Inhalten einsetzen.

Sie können mithilfe der Status- und Protokolldaten Berichte und Statusinformationen für alle Blades erhalten. Mit dem Management-Blade-Server können Sie DAT-Dateien auf allen Blade-Servern zum Scannen von Inhalten auf dem neuesten Stand halten und darüber hinaus den Quarantäne-Speicherort verwalten.

Blade-Server-Statusinformationen

Während der Datenverkehr den Blade-Server passiert, können Sie das Dashboard aufrufen, um aktuelle Informationen zum Gesamtdatendurchsatz, zu Erkennungen und zur Leistung für die einzelnen Protokolle zu erhalten.

Das Dashboard enthält die folgenden Blade-spezifischen Informationen:

- **Allgemeiner Status** (Management-Blade-Server und Failover-Management-Blade-Server)
- **Hardware-Status** (Management-Blade-Server)
- **Blade-Status** (alle Blades)

Diese Tabelle zeigt die Informationen an, die Sie zu allen Blades erhalten können.

Geschwindigkeitsmesser	Der durchschnittliche Durchsatz des Blade-Servers auf der Grundlage der alle paar Minuten vorgenommenen Messungen.
Name	Name des Blades: • Der Management-Blade-Server. • Der Failover-Management-Blade-Server. Diese Namen werden mithilfe der Konfigurationskonsole angegeben. • Blade <Nummer> – Blade-Server zum Scannen von Inhalten.
Status	Der aktuelle Status der einzelnen Blades.
Auslastung	Die Gesamtsystemauslastung für jedes Blade.
Aktiv	Die Anzahl der derzeit auf jedem Blade aktiven Verbindungen. Die Zeile für den Management-Blade-Server zeigt die Gesamtzahl für alle Blade-Server zum Scannen von Inhalten an.
Verbindungen	Die Gesamtzahl der Verbindungen seit dem letzten Zurücksetzen der Zähler. Die Zeile für den Management-Blade-Server zeigt die Gesamtzahl für alle Blade-Server zum Scannen von Inhalten an.
Weitere Spalten	Versionsinformationen für das Antiviren-Modul, die Antiviren-DAT-Dateien, das Anti-Spam-Modul und die Anti-Spam-Regeln. Wenn die Blades auf dem aktuellen Stand sind, stimmen die Versionsnummern überein. Während der Aktualisierung können die Werte voneinander abweichen.

Generieren von Berichten

McAfee Email Gateway Blade Server enthält mehrere vordefinierte Berichte, die Sie im PDF-, HTML- oder Textformat herunterladen können. Sie können den Zeitplan für die Erstellung dieser Berichte definieren und angeben, an wen die Berichte gesendet werden sollen. Sie können auch eigene Berichte erstellen.

Das Blade-Server-Protokoll zeigt Ereignisinformationen für den ausgewählten Berichttyp und den ausgewählten Zeitraum an. Mit den Berichtsfunktionen des Blade-Servers können Sie Berichte erstellen oder Protokolle, Statistiken, Leistungsindikatoren und Diagramme für eine Vielzahl von Daten zum Blade-Server und seinen Aktivitäten anzeigen, beispielsweise die Arbeitsspeicher- und Prozessorauslastung.

Klicken Sie beispielsweise, nachdem Sie die Schritte unter *Testen von E-Mail-Verkehr und Virenentdeckung* ausgeführt haben, auf **Berichte** | **Nachrichtensuche**. Die erkannte EICAR-Testdatei wird angezeigt.

Weitere Berichtsinformationen

Sie haben folgende Möglichkeiten:

- Speichern Sie den Bericht unter **Favoriten**. Dies ermöglicht Ihnen, denselben Bericht in der Zukunft auszuführen.
- Wechseln Sie, wenn relevant, zwischen verschiedenen Ansichten der Berichtsdaten.

Gehen Sie wie nachfolgend beschrieben vor, um die DAT-Dateien des Blade-Servers zu aktualisieren und anschließend den Aktualisierungsbericht zu lesen.

Vorgehensweise

1. Wählen Sie **System** | **Komponentenverwaltung** | **Aktualisierungsstatus**.
2. Klicken Sie unter **Versionsinformationen und Aktualisierungen** für sämtliche Antiviren- oder Anti-Spam-DAT-Dateiaktualisierungen, die Sie aktualisieren möchten, auf **Jetzt aktualisieren**.
3. Wählen Sie **Berichte** | **E-Mail-Berichte** | **Auswahl** | **Filter**.
4. Klicken Sie auf **Übernehmen**.

   Es werden Informationen zu den Aktualisierungen angezeigt, die auf Ihrem Blade-Server installiert wurden.

Verwenden von Richtlinien für die Verwaltung von Nachrichten-Scans

Erleben Sie die Scan-Funktionen des Blade-Servers in Aktion. Sie werden detailliert durch das Erstellen und Testen einiger Beispielrichtlinien geführt und erfahren, wie Sie die relevanten Berichte generieren.

Eine Richtlinie ist eine Zusammenstellung von Einstellungen und Regeln, die dem Blade-Server mitteilt, wie er bestimmte Gefahren für Ihr Netzwerk abwehren soll. Wenn Sie Echtzeitscan-Richtlinien für Ihr Unternehmen erstellen, müssen Sie Ihre Anforderungen in Ruhe analysieren und planen. Sie finden Hinweise für die Richtlinienplanung in der Online-Hilfe.

Vor dem Erstellen von Richtlinien

Konfigurieren Sie vor dem Erstellen der Richtlinien McAfee Email Gateway Blade Server zur Verwendung von McAfee Quarantine Manager.

Alle Quarantäneaktionen sind standardmäßig deaktiviert. Bevor Sie sie aktivieren, konfigurieren Sie den Blade-Server so, dass der Quarantäne-Speicherort unter Verwendung von McAfee Quarantine Manager verwaltet wird.

Vorgehensweise

1. Wählen Sie in der Benutzeroberfläche **E-Mail** | **Quarantäne-Konfiguration**.
2. Wählen Sie **Off-Box-McAfee Quarantine Manager (MQM)-Dienst verwenden**.
3. Geben Sie nähere Informationen zu Ihrem McAfee Quarantine Manager ein.

   Wenn Sie eine vorhandene McAfee-Appliance durch einen McAfee Email Gateway Blade Server ersetzen, stellen Sie sicher, dass Sie Ihre bestehende **Appliance-ID** verwenden. Mit einer abweichenden **Appliance-ID** ist es nicht möglich, Nachrichten freizugeben, die von der alten Appliance isoliert wurden.

4. Übernehmen Sie Ihre Änderungen.

Erstellen einer Antiviren-Scan-Richtlinie

Antiviren-Richtlinien ermöglichen es Ihnen, Ihren Schutz vor Viren und Malware zu optimieren.

Eine Antiviren-Scan-Richtlinie soll folgende Aktionen umfassen:

- Viren in eingehenden Nachrichten erkennen
- Die Original-E-Mail isolieren
- Den Empfänger benachrichtigen
- Den Absender warnen

Gehen Sie wie nachfolgend beschrieben vor, um zu zeigen, was passiert, wenn eine Mass-Mailer-Virenregel durch die EICAR-Testdatei ausgelöst wird, und welche Aktionen durchgeführt werden können.

Vorgehensweise

1 Stellen Sie auf dem Blade-Server sicher, dass Sie McAfee Quarantine Manager verwenden (**E-Mail** | **Quarantäne-Konfiguration** | **Quarantäneoptionen**).

2 Wählen Sie auf dem Gerät **Email** | **Email Policies** | **Anti-Virus**.

Die Standardrichtlinie wird auf **Säubern oder durch Warnung ersetzen** gesetzt, wenn das Säubern fehlschlägt.

3 Klicken Sie auf **Viren: Säubern oder durch Warnung ersetzen**, um die **Standardeinstellungen für Anti-Virus (SMTP)** anzuzeigen.

4 Stellen Sie unter **Aktionen** im Bereich **Wenn ein Virus erkannt wird** sicher, dass **Säuberung versuchen** ausgewählt ist.

5 Wählen Sie im Abschnitt **Und auch** unter der Aktion die Optionen **Benachrichtigungs-E-Mail an Absender zustellen** und **Isolieren der ursprünglichen E-Mail** aus.

6 Wählen Sie unter **Wenn das Säubern fehlschlägt** die Option **Erkanntes Element durch Warnung ersetzen** aus.

7 Wählen Sie im Abschnitt **Und auch** unter **Wenn das Säubern fehlschlägt** die Optionen **Benachrichtigungs-E-Mail an Absender zustellen** und **Isolieren der ursprünglichen E-Mail** als sekundäre Aktionen aus.

8 Klicken Sie auf **OK**.

9 Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien [Scanner-Optionen] – Konfiguration der E-Mail-Adresse**.

10 Weisen Sie unter **Gebouncte E-Mails** die E-Mail-Adresse als Administrator-E-Mail-Adresse zu.

Ohne diese Konfiguration fügt das Gerät keine Absenderadresse zur E-Mail-Benachrichtigung hinzu. Die meisten E-Mail-Server stellen keine E-Mails ohne Absenderadresse zu.

11 Klicken Sie auf **OK** und anschließend auf das grüne Häkchen.

12 Wählen Sie **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien [Antivirus] | Benutzerdefinierte Malware-Optionen**.

13 Wählen Sie **Mass-Mailer**, und setzen Sie anschließend **Bei Erkennung** auf **Verbindung verweigern (Blockieren)**.

Der Absender-E-Mail-Server empfängt die Fehlermeldung **Code 550: denied by policy** (Durch Richtlinie verweigert). Das Gerät verwaltet eine Liste der Verbindungen, die unter keinen Umständen E-Mails senden dürfen. Die Liste kann unter **E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Listen für Zulassen und Verweigern [+] Zugelassene und blockierte Verbindungen** angezeigt werden. Die Option **Verweigerte Verbindungen** ist in der Online-Hilfe beschrieben.

14 So testen Sie die Konfiguration:

   a Senden Sie eine E-Mail von <Client-E-Mail-Adresse> an <Server-E-Mail-Adresse>.

   b Erstellen Sie eine Textdatei, die folgende Zeichenfolge enthält:

   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

   c Speichern Sie die Datei als eicar.txt.

   d Hängen Sie die Datei an die E-Mail an.

   Das E-Mail-Gateway ersetzt die Datei durch eine Warnung, und der Absender wird über den Vorgang benachrichtigt.

15 Kehren Sie zu **Benutzerdefinierte Malware-Optionen** zurück, und klicken Sie auf **Spezifischer Erkennungsname:**.

16 Geben Sie EICAR ein.

17 Stellen Sie sicher, dass als primäre Aktion **Daten zurückweisen und Fehlercode zurückgeben (Blockieren)** festgelegt ist, und klicken Sie anschließend auf **OK**.

18 Erstellen Sie von einem externen E-Mail-Konto aus eine Nachricht, und hängen Sie die EICAR-Testdatei an.

   Der E-Mail-Client gibt folgende Fehlermeldung zurück: **550: durch Richtlinie verweigert. E-Mail | E-Mail-Konfiguration | Empfangen von E-Mails | Listen für Zulassen und Ablehnen [+] Blockierte Verbindungen** ist leer.

19 Ändern Sie unter **Benutzerdefinierte Malware-Optionen** die primäre Aktion in **Verbindung verweigern**, und klicken Sie anschließend auf **OK**.

20 Senden Sie die E-Mail, und überprüfen Sie die verweigerte Verbindung. Sie weist die IP-Adresse Ihres Client-Computers (Beispiel-IP-Adresse) auf.

21 Senden Sie nun eine reguläre E-Mail. Diese wird aufgrund der Liste der verweigerten Verbindungen ebenfalls abgelehnt. Für den Absender-Server scheint es, als ob der Server nicht online wäre.

Das Gerät prüft die Nachricht, wenn diese auf dem E-Mail-Gateway eingeht, und erkennt, dass sie einen Virus enthält. Die Nachricht wird isoliert, und die vorgesehenen Empfänger und der Absender werden darüber benachrichtigt, dass die Nachricht infiziert war.

Erstellen einer Anti-Spam-Scan-Richtlinie

Richten Sie eine Richtlinie zum Schutz Ihres Unternehmens vor dem Empfang unerwünschter Nachrichten ein.

Bevor Sie beginnen

Eine solche Richtlinie schützt Benutzer vor dem Empfang unerwünschter E-Mail-Nachrichten, die ihre Produktivität senken und den Nachrichtenverkehr über Ihre Server erhöhen.

Vorgehensweise

1 Stellen Sie auf dem Blade-Server sicher, dass Sie McAfee Quarantine Manager verwenden (**E-Mail | Quarantäne-Konfiguration | Quarantäneoptionen**).

2 Wählen Sie **Email | Email Policies**.

   Sie müssen für die SMTP- und POP3-Protokolle jeweils eine separate Anti-Spam-Richtlinie einrichten.

3 Legen Sie die primäre Aktion auf **Daten akzeptieren und verwerfen** fest.

4 Legen Sie die sekundäre Aktion auf **Original-E-Mail isolieren** fest. Ändern Sie den Spam-Faktor auf 5.

Wenn Sie die Spam-Erkennung aktivieren, empfiehlt McAfee, auch die Phishing-Erkennung zu aktivieren. Die Scan-Leistung wird durch das gleichzeitige Ausführen von Anti-Spam- und Anti-Phishing-Tests nicht beeinträchtigt.

Erstellen einer Compliance-Richtlinie

Erstellen Sie eine Richtlinie für die Isolierung eingehender Nachrichten, die unerwünschten Inhalt enthalten.

Dies erfolgt nun mithilfe eines Assistenten, der Sie durch den Vorgang führt.

Gehen Sie wie folgt vor, um eine Compliance-Richtlinie einzurichten:

Vorgehensweise

1 Wählen Sie auf dem Gerät **E-Mail** | **DLP und Compliance** | **Compliance-Wörterbücher**.

2 Wählen Sie **E-Mail-Wörterbuchliste** aus.

3 Zeigen Sie den Bereich **Wörterbuchdetails für ...** an.

4 Wählen Sie **Email** | **Email Policies** | **Compliance**.

5 Wählen Sie **Compliance**.

6 Wählen Sie **Compliance aktivieren** | **Ja** aus.

7 Klicken Sie auf **OK**.

8 Klicken Sie unter **Regeln** auf **Neue Regel erstellen**.

9 Geben Sie einen Namen für die Regel ein.

10 Klicken Sie auf **Weiter**.

11 Wählen Sie unter **Einzubeziehende Wörterbücher** die gewünschten Wörterbücher aus. Wählen Sie für diesen Test finanzbezogene Wörterbücher aus.

12 Klicken Sie auf **Weiter**.

13 Wählen Sie unter **Auszuschließende Wörterbücher** die gewünschten Wörterbücher aus.

14 Wählen Sie die durchzuführenden Aktionen aus.

15 Erstellen Sie eine E-Mail auf dem Server von <Beispiel-Server-E-Mail-Adresse> an <Beispiel-Client-E-Mail-Adresse>. Geben Sie folgenden Text ein: Hallo: Wir müssen den bestätigten Wert Ihrer Rente berechnen. Falls sich herausstellt, dass Ihre Anlagen über weniger Kapital verfügen als erwartet, sollten Sie eine Schlichtungsstelle anrufen.

16 Senden Sie die Nachricht.

17 Verwenden Sie **Berichte** | **Nachrichtensuche**, um die Ergebnisse anzuzeigen.

Der Client-E-Mail-Agent erhält die E-Mail nicht. Das Server-E-Mail-Konto sollte zwei E-Mail-Nachrichten erhalten: eine E-Mail-Benachrichtigung, dass die Nachricht den Compliance-Test nicht bestanden hat, und eine Kopie der ursprünglichen E-Mail.

Informationen zum Verwalten virtueller Hosts

Bei der Verwendung von virtuellen Hosts kann sich ein einzelnes Gerät wie mehrere Geräte verhalten.

Jedes virtuelle Gerät kann den Datenverkehr innerhalb von angegebenen IP-Adressbereichen verwalten, was dem Gerät ermöglicht, Scan-Dienste für den Datenverkehr von vielen Quellen oder Kunden anzubieten.

Vorzüge

- Trennt den Datenverkehr der einzelnen Kunden voneinander.
- Für jeden Kunden oder Host können Richtlinien erstellt werden, was die Konfiguration vereinfacht und Konflikte verhindert, die bei komplexen Richtlinien auftreten können.
- Berichte sind für jeden Kunden oder Host einzeln verfügbar, wodurch die Notwendigkeit einer komplexen Filterung entfällt.
- Falls das Gerät verhaltensbedingt auf eine Reputation-Blacklist gesetzt wird, betrifft dies nur einen virtuellen Host und nicht das gesamte Gerät.

Einrichten der virtuellen Hosts

Die Funktion steht nur für SMTP-Scans zur Verfügung. Informationen zur Angabe des Pools der IP-Adressen für den eingehenden Datenverkehr und des optionalen Pools der Adressen für den ausgehenden Datenverkehr finden Sie auf den Seiten **System | Virtuelles Hosting | Virtuelle Hosts** und **System | Virtuelles Hosting | Virtuelle Netzwerke**.

Verwalten der virtuellen Hosts

Funktion	Verhalten
E-Mail-Richtlinie	Jeder virtuelle Host besitzt eine eigene Registerkarte, auf der Sie die Scan-Richtlinien für den Host erstellen können.
E-Mail-Konfiguration	Jeder virtuelle Host besitzt eine eigene Registerkarte, auf der Sie spezielle MTA-Funktionen für den jeweiligen Host konfigurieren können.
E-Mail in der Warteschlange	Sie können alle in der Warteschlange befindlichen E-Mails oder nur die in der Warteschlange befindlichen E-Mails für die einzelnen Hosts anzeigen.
Isolierte E-Mails	Sie können alle isolierten E-Mails oder nur die isolierten E-Mails für die einzelnen Hosts anzeigen.
Berichterstellung	Sie können alle Berichte oder nur die Berichte für die einzelnen Hosts anzeigen.

Verhalten zwischen dem Gerät und MTAs

Wenn das Gerät E-Mails empfängt, die an den IP-Adressbereich des virtuellen Hosts gesendet wurden, führt der virtuelle Host Folgendes aus:

- Er reagiert mit einem eigenen SMTP-Willkommensbanner auf die SMTP-Konversation.
- Er fügt optional seine eigenen Adressinformationen zum Header "Received" hinzu.
- Er scannt die E-Mails gemäß seiner eigenen Richtlinie.

Wenn das Gerät E-Mails zustellt, geschieht Folgendes:

- Die IP-Adresse wird einem Adresspool für ausgehenden Datenverkehr entnommen, oder es wird eine physische IP-Adresse verwendet, wenn kein entsprechender Adresspool angegeben wurde.
- Der empfangende Mailübertragungsagent (MTA) sieht die IP-Adresse des virtuellen Hosts.

- Wenn ein Adresspool vorhanden ist, wird die IP-Adresse nach dem Round-Robin-Verfahren ausgewählt.
- Die EHLO-Antwort wird an den virtuellen Host ausgegeben.

Testen der Konfiguration

Erfahren Sie, wie Sie anhand eines Tests feststellen können, ob McAfee Email Gateway Blade Server nach der Installation ordnungsgemäß funktioniert.

McAfee empfiehlt, die Bereiche System-, Netzwerk- und Hardware-Zusammenfassung des **Dashboards** bei der ersten Anmeldung am Blade-Server auf empfohlene Konfigurationsänderungen zu überprüfen.

Testen der Verbindung

Stellen Sie sicher, dass Sie über eine Verbindung zu und von Ihrem Blade-Server verfügen.

Der Blade-Server prüft, ob er mit dem Gateway, den Update-Servern und den DNS-Servern kommunizieren kann. Außerdem wird bestätigt, dass der Name und der Domänenname gültig sind.

Vorgehensweise

1 Öffnen Sie die Seite **Systemtests** mit einer der folgenden Methoden:
   - Wählen Sie im Bereich **Tasks** des **Dashboards** die Option **Systemtests ausführen**.
   - Wählen Sie in der Navigationsleiste die Option **Fehlerbehebung**.

2 Klicken Sie auf die Registerkarte **Tests**.

3 Klicken Sie auf **Tests starten**. Verifizieren Sie, dass alle Tests erfolgreich abgeschlossen wurden.

Aktualisieren der DAT-Dateien

Sobald Sie die Konfigurationskonsole ausgeführt haben, versucht McAfee Email Gateway Blade Server, alle aktivierten Scanner zu aktualisieren.

Gehen Sie wie nachfolgend beschrieben vor, um sicherzustellen, dass Ihr Blade-Server über die aktuellsten Erkennungsdefinitionsdateien (DAT) verfügt.

Im Rahmen der Verwendung von McAfee Email Gateway Blade Server können Sie einzelne Arten von Definitionsdateien aktualisieren sowie die standardmäßig geplanten Aktualisierungen an Ihre Anforderungen anpassen.

Sie können den Aktualisierungsstatus Ihres McAfee Email Gateway Blade Server überprüfen, indem Sie das Portlet **Dienste** im **Dashboard** anzeigen.

Vorgehensweise

1 Wählen Sie zum Öffnen der Seite **Aktualisierungen** die Optionen **System** | **Komponentenverwaltung** | **Aktualisierungsstatus**.

2 Wenn Sie alle DAT-Dateien aktualisieren möchten, klicken Sie neben der Antiviren-Modul-Komponente auf **Jetzt aktualisieren**.

Testen von E-Mail-Verkehr und Virenerkennung

Gehen Sie wie nachfolgend beschrieben vor, um zu überprüfen, ob E-Mail-Verkehr erfolgreich durch Ihren Blade-Server geleitet wird und Bedrohungen ordnungsgemäß identifiziert werden.

McAfee verwendet die EICAR-Testdatei (European Expert Group for IT-Security), eine harmlose Datei, die eine Virenerkennung auslöst.

Vorgehensweise

1. Senden Sie eine E-Mail von einem externen E-Mail-Konto (wie Hotmail) an einen internen Posteingang, und vergewissern Sie sich, dass die E-Mail angekommen ist.
2. Sehen Sie sich **Berichte** | **Nachrichtensuche** an. Aus der Liste für das Protokoll, das Sie zum Versenden der Nachricht verwendet haben, sollte hervorgehen, dass eine Nachricht empfangen wurde.
3. Kopieren Sie die folgende Zeile in eine Datei, und achten Sie dabei darauf, dass Sie keine Leerzeichen oder Zeilenumbrüche hinzufügen: X5O!P %@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARDANTIVIRUS-TEST-FILE!$H+H*
4. Speichern Sie die Datei unter dem Namen EICAR.COM.
5. Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine Nachricht mit der Datei EICAR.COM als Anhang, und senden Sie die Nachricht an einen internen Posteingang.
6. Wählen Sie **Berichte** | **Nachrichtensuche**. Sie sollten sehen, dass ein Virus erkannt wurde.
7. Löschen Sie die Nachricht, wenn Sie das Testen Ihrer Installation abgeschlossen haben, damit ahnungslose Benutzer keinen Schreck bekommen.

Testen der Spam-Erkennung

Führen Sie einen "General Test mail for Unsolicited Bulk Email" (Allgemeinen Test auf unerwünschte Bulk-E-Mails – GTUBE) aus, mit dem geprüft wird, ob eingehender Spam erkannt wird.

Vorgehensweise

1. Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine neue E-Mail.
2. Kopieren Sie den folgenden Text in den Nachrichtenteil der E-Mail:

   XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARDANTI-UBE-TEST-EMAIL*C.34X

   Vergewissern Sie sich, dass Sie keine Leerzeichen oder Zeilenumbrüche eingeben.
3. Senden Sie die neue E-Mail an eine interne Posteingangsadresse. Die Software scannt die Nachricht, erkennt sie als Junk-E-Mail und verarbeitet sie entsprechend. Der GTUBE-Test hat Vorrang vor Blacklists und Whitelists.

Erkunden der McAfee Email Gateway Blade Server-Funktionen

Erleben Sie die Scan-Funktionen von McAfee Email Gateway Blade Server in Aktion.

Gehen Sie wie nachfolgend beschrieben vor, und lassen Sie sich Schritt für Schritt durch das Erstellen und Testen einiger Beispielrichtlinien und das Generieren relevanter Berichte führen.

Scan-Richtlinien und deren Einfluss auf Ihr Netzwerk

Eine Richtlinie ist eine Zusammenstellung von Einstellungen und Regeln, die McAfee Email Gateway Blade Server mitteilen, wie bestimmte Gefahren für Ihr Netzwerk abgewehrt werden sollen.

Wenn Sie Echtzeitscan-Richtlinien für Ihr Unternehmen erstellen, müssen Sie Ihre Anforderungen in Ruhe analysieren und planen.

Hinweise für die Richtlinienplanung finden Sie in der Online-Hilfe, die über die Produktbenutzeroberfläche aufgerufen werden kann.

Inhaltsscans unter Verwendung der E-Mail-Compliance-Regeln

Verwenden Sie Compliance-Scans zur Unterstützung der Compliance mit gesetzlichen und betrieblichen Auflagen.

Sie können aus einer Bibliothek aus vordefinierten Compliance-Regeln wählen oder eigene Regeln und Wörterbücher für Ihr Unternehmen erstellen.

Compliance-Regeln können hinsichtlich ihrer Komplexität von einem einfachen Auslöser bei der Erkennung eines einzelnen Begriffs in einem Wörterbuch bis hin zum Aufbauen auf und Kombinieren von faktorbasierten Wörterbüchern variieren, die nur auslösen, wenn ein bestimmter Schwellenwert erreicht wird. Mithilfe der erweiterten Funktionen von Compliance-Regeln können Wörterbücher mit den logischen Operationen eines von, alle von oder außer kombiniert werden.

Vorgehensweise

1 Gehen Sie wie folgt vor, um E-Mail-Nachrichten zu blockieren, die die Richtlinie "Bedrohliche Sprache" verletzen:

   a Navigieren Sie zu **Email** | **Email Policies**, und wählen Sie **Compliance**.

   b Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

   c Klicken Sie auf **Neue Regel aus Vorlage erstellen**, um den **Assistent für die Regelerstellung** zu öffnen.

   d Wählen Sie die Richtlinie **Zulässige Nutzung - Bedrohliche Sprache** aus, und klicken Sie auf **Weiter**.

   e Sie können den Namen der Regel optional ändern. Klicken Sie anschließend auf **Weiter**.

   f Ändern Sie die primäre Aktion in **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **Fertig stellen**.

   g Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

2 Gehen Sie wie folgt vor, um eine einfache benutzerdefinierte Regel zum Blockieren von E-Mail-Nachrichten zu erstellen, die Sozialversicherungsnummern enthalten:

   a Navigieren Sie zu **Email** | **Email Policies**, und wählen Sie **Compliance**.

   b Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

   c Klicken Sie auf **Neue Regel erstellen**, um den **Assistenten für die Regelerstellung** zu öffnen.

   d Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.

   e Geben Sie im **Suchfeld** *sozial* ein.

   f Wählen Sie das Wörterbuch **Sozialversicherungsnummer** aus, und klicken Sie zweimal auf **Weiter**.

   g Wählen Sie die Aktion **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **Fertig stellen**.

3 Gehen Sie wie folgt vor, um eine komplexe Regel zu erstellen, die auslöst, wenn sowohl Wörterbuch A als auch Wörterbuch B erkannt werden, jedoch nicht, wenn darüber hinaus auch Wörterbuch C erkannt wird:

   a Navigieren Sie zu **Email** | **Email Policies**, und wählen Sie **Compliance**.

   b Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

   c Klicken Sie auf **Neue Regel erstellen**, um den **Assistenten für die Regelerstellung** zu öffnen.

   d Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.

e Wählen Sie zwei Wörterbücher aus, die in die Regel aufgenommen werden sollen, und klicken Sie auf **Weiter**.

f Wählen Sie in der Ausschlussliste ein Wörterbuch aus, das Sie von der Regel ausschließen möchten.

g Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn die Regel ausgelöst wird.

h Wählen Sie im Dropdown-Feld **Und bedingt** die Option **Alle** aus, und klicken Sie auf **Fertig stellen**.

4 Gehen Sie wie folgt vor, um ein neues Wörterbuch zu einer vorhandenen Regel hinzuzufügen:

a Navigieren Sie zu **Email** | **Email Policies**, und wählen Sie **Compliance**.

b Erweitern Sie die Regel, die Sie bearbeiten möchten.

c Wählen Sie **Wörterbuch hinzufügen**.

d Wählen Sie das neue Wörterbuch aus, das Sie hinzufügen möchten, und klicken Sie auf **OK**.

5 Gehen Sie wie folgt vor, um eine "Unzufriedenheit"-Regel zu konfigurieren, die mit einem niedrigen Schwellenwert überwacht wird und bei einem hohen Schwellenwert blockiert:

a Navigieren Sie zu **Email** | **Email Policies**, und wählen Sie **Compliance**.

b Klicken Sie auf **Neue Regel erstellen**, geben Sie einen Namen für die Regel ein, beispielsweise *Unzufriedenheit - Niedrig*, und klicken Sie auf **Weiter**.

c Wählen Sie das Wörterbuch **Unzufriedenheit** aus, und geben Sie unter **Schwellenwert** den Wert *20* ein.

d Klicken Sie auf **Weiter** und anschließend erneut auf **Weiter**.

e Akzeptieren Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Standardaktion.

f Klicken Sie auf **Fertig stellen**.

g Wiederholen Sie die Schritte 2 bis 4, um eine weitere neue Regel zu erstellen. Nennen Sie diese jedoch *Unzufriedenheit – Hoch*, und weisen Sie ihr den Schwellenwert *40* zu.

h Wählen Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Option **Daten akzeptieren und anschließend verwerfen (Blockieren)** aus.

i Klicken Sie auf **Fertig stellen**.

j Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

Vermeiden des Verlusts vertraulicher Daten

Erfahren Sie, wie Sie das Versenden eines vertraulichen Finanzdokuments aus Ihrem Unternehmen heraus blockieren können.

Vorgehensweise

1 Navigieren Sie zu **E-Mail** | **DLP und Compliance** | **Registrierte Dokumente**, und erstellen Sie die Kategorie **Finanzen**.

2 Navigieren Sie zu **Email** | **Email Policies**, und wählen Sie die Richtlinie **Schutz vor Datenverlust**.

3 Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.

4 Klicken Sie auf **Neue Regel erstellen**, wählen Sie die Kategorie **Finanzen** aus, und klicken Sie auf **OK** damit die Kategorie in der Liste "Regeln" angezeigt wird.

5 Wählen Sie die der Kategorie zugeordnete Aktion aus, ändern Sie die primäre Aktion in **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **OK**.

6 Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

Informationen zu isolierten E-Mail-Nachrichten

Der McAfee Email Gateway Blade Server verwendet die Software McAfee Quarantine Manager und stellt damit eine Off-Box-Quarantänelösung für Ihre E-Mail-Nachrichten bereit.

Nähere Informationen dazu, wo Sie die isolierten Nachrichten finden, entnehmen Sie der Dokumentation zu McAfee Quarantine Manager.

Überwachen der Spam-Erkennung

Überwachen Sie die Spam-Erkennungsrate mit der standardmäßigen SMTP-Spam-Erkennungsrichtlinie.

Sobald Sie die Konfigurationskonsole ausgeführt haben, funktionieren diese Einstellungen und schützen Ihr Netzwerk und Ihre Benutzer vor unerwünschten Spam-Nachrichten. Eine ausführlichere Erläuterung der Einstellungen finden Sie in der Online-Hilfe, die über die Benutzeroberfläche aufgerufen werden kann.

Standardmäßig gilt für McAfee Email Gateway Blade Server folgende Aufgaben aus:

- Phishing-Nachrichten werden blockiert.
- Nachrichten mit einer Einstufung von mindestens fünf werden als Spam markiert.
- Spam-Nachrichten mit einer Einstufung von mindestens zehn werden verworfen.
- Die Absenderauthentifizierung ist aktiviert. Mithilfe dieser Standardeinstellungen erkennt McAfee Email Gateway Blade Server mehr als 98 Prozent aller Spam-Nachrichten.

Die Absenderauthentifizierung umfasst die McAfee Global Threat Intelligence-Nachrichten-Reputation. Wenn ein Absender die Überprüfung der McAfee Global Threat Intelligence-Nachrichten-Reputation nicht besteht, weist der Blade-Server die Nachricht zurück, beendet die Verbindung und lässt die IP-Adresse des Absenders nicht mehr zu. Die IP-Adresse des Absenders wird zu einer Liste blockierter Verbindungen hinzugefügt und automatisch zehn Minuten lang auf Kernel-Ebene blockiert (die standardmäßige Blockierdauer kann geändert werden). In den Bereichen **SMTP-Entdeckungen** und **POP3-Entdeckungen** des **Dashboards** wird die Anzahl der blockierten Verbindungen angezeigt.

Vorgehensweise

1 Wählen Sie **Email** | **Email Policies** | **Spam**, um die Standardeinstellungen für die Spam-Erkennung anzuzeigen.

2 Vergewissern Sie sich, dass Spam-Nachrichten ordnungsgemäß identifiziert werden, indem Sie eine Nachricht McAfee Email Gateway Blade Server passieren lassen, bei der die Einstellungen zur Spam-Entdeckung ausgelöst werden.

3 Wenn Sie die Entdeckungsrate überwachen möchten, kehren Sie zum **Dashboard** zurück, und betrachten Sie die Bereiche **SMTP-Entdeckungen** und **POP3-Entdeckungen**.

Die Zahl für **Spam und Phishing** und für **Absenderauthentifizierung** wird hochgezählt. Die Zahl für die Absenderauthentifizierungsentdeckungen beinhaltet die Anzahl der Absender, welche die Überprüfung der McAfee Global Threat Intelligence-Nachrichten-Reputation nicht bestanden haben. E-Mail-Diagramme bieten eine grafische Darstellung der Daten.

4 Wenn Sie einen Bericht über die E-Mail-Aktivität erhalten möchten, navigieren Sie zu **Berichte** | **E-Mail-Berichte** | **Auswahl** | **Favoriten**, und wählen Sie **Bevorzugte E-Mail-Berichte anzeigen**.

5 Sehen Sie sich die Berichte **Blockiert (letzte 24 Stunden)** und **Häufigste Spam-Absender (letzte 24 Stunden)** an.

4 Betrieb im ausfallsicheren Modus

McAfee Email Gateway Blade Server umfasst den Betrieb im ausfallsicheren Modus für den Blade-Server.

In diesem Modus werden alle Verbindungen zwischen Ihrem Netzwerk und dem Blade-Server sowie die Verbindungen innerhalb des Blade-Server-Gehäuses so ausgelegt, dass mehrere Pfade verwendet werden können.

Auf diese Weise kann der Ausfall von Serverkomponenten, Netzwerkgeräten oder Verkabelung, die für Weiterleitung des Datenverkehrs zwischen Ihrem Netzwerk und dem Blade-Server verwendet werden, besser verkraftet werden.

Inhalt

- *Nutzung der Hardware im ausfallsicheren Modus*
- *Entscheidung für die Verwendung des ausfallsicheren Modus*
- *Vor dem Umkonfigurieren in den ausfallsicheren Modus*
- *Aktivieren des ausfallsicheren Modus*
- *Konfigurieren der Interconnect-Module*
- *Ändern der Gehäusekonfiguration*
- *Anwenden der Konfiguration für den ausfallsicheren Modus auf alle Interconnect-Module*
- *Konfigurieren des Management-Blade-Servers für den ausfallsicheren Modus*
- *Verbindungen zum externen Netzwerk im ausfallsicheren Modus*
- *Einschalten der Blades*

Nutzung der Hardware im ausfallsicheren Modus

Im ausfallsicheren Modus wird die Blade-Server-Hardware anders als im Standardmodus (nicht ausfallsicher) verwendet.

Im ausfallsicheren Modus werden die Netzwerkverbindungen in folgende Segmente innerhalb und außerhalb des Blade-Server-Gehäuses aufgeteilt:

- LAN1 und LAN2 werden für Verbindungen mit externen Netzwerken zur Übertragung des gescannten Datenverkehrs genutzt. Diese werden entweder für getrennte Netzwerke (in den Modi „Expliziter Proxy" oder „Transparenter Router") oder für die beiden Anschlüsse im Modus „Transparente Bridge" verwendet.

  Der gescannte Datenverkehr wird immer über alle aktiven Interconnect-Module übertragen, um einen maximalen Durchsatz und maximale Ausfallsicherheit zu gewährleisten.

- Das Out of Band-Netzwerk (OOB) ermöglicht es, den Datenverkehr für die Verwaltung vom gescannten Datenverkehr getrennt zu halten. Wenn es eingesetzt wird, kann das System so konfiguriert werden, dass keine Verwaltungsarbeiten über die LAN1- und LAN2-Netzwerke erfolgen können.

  Das OOB-Netzwerk wird über das LAN2-Interconnect-Modul auf einem getrennten VLAN mit getrennten Switch-Verbindungen übertragen.

  Das OOB-Netzwerk kann alternativ über ein VLAN-Netzwerk auf denselben externen Anschlüssen der Interconnect-Module LAN1 und LAN2 übertragen werden.

- Der Datenverkehr zwischen den Management-Blade-Servern und den Scan-Blades wird auf einem separaten VLAN innerhalb des Blade-Server-Gehäuses abgewickelt. Dabei handelt es sich um ein privates VLAN innerhalb des Gehäuses, das normalerweise außerhalb des Gehäuses nicht zur Verfügung steht.

  Das Scanning-VLAN ist auf den Management-Blade-Servern gekennzeichnet, auf den Scan-Blades jedoch nicht gekennzeichnet. Dadurch funktioniert die PXE-Installation (Preboot Execution Environment) der Scan-Blades wie erwartet.

  Die Konfiguration der Interconnect-Module ist für Management-Blade-Server und Scan-Blades unterschiedlich. McAfee empfiehlt, dass Sie nur die in diesem Dokument empfohlenen Blade-Steckplätze für die Management- und Scan-Blades verwenden, um Konfigurationsprobleme zu vermeiden.

Im Gehäuse werden vier Interconnect-Module verwendet, um eine Ausfallsicherheit im Falle des Ausfalls einer der oben beschriebenen Netzwerkverbindungen zu gewährleisten. Die Ausfallsicherheit ist bei folgenden Ausfällen gegeben:

- Ausfall einer externen Verbindung

  Die Ausfallsicherheit bei externen Verbindungen wird durch die Unterstützung von aggregierten Verbindungen (auch als Bonding, Trunking, Port Channel oder Etherchannel bezeichnet) ermöglicht. Es können bis zu fünf Verbindungen gebündelt werden, um eine maximale Ausfallsicherheit zu erreichen. Vom Ausfall einer einzelnen Verbindung sind nur die Pakete betroffen, die zum Zeitpunkt des Ausfalls über die jeweilige Verbindung übertragen werden. Das Interconnect-Modul und die benachbarte Infrastruktur stoppen automatisch die Nutzung der ausgefallenen Verbindung.

- Ausfall einer internen Verbindung

  Intern werden Querverbindungspaare verwendet, um eine redundante Konnektivität zwischen benachbarten Interconnect-Modulen zu gewährleisten. Dies bedeutet, dass beim Ausfall aller Verbindungen im Blade-Gehäuse, die extern zum

  Interconnect-Modul sind, der Datenverkehr weiterhin über das benachbarte Interconnect-Modul und über die Querverbindung zum Original-Blade erfolgen kann. Vom Ausfall einer Verbindung sind nur die Pakete betroffen, die zum Zeitpunkt des Ausfalls über die jeweilige Verbindung übertragen werden. STP wird zur Vermeidung von Netzwerk-Loops verwendet.

- Ausfall einer Blade-Netzwerkkarte

  Alle Blades verfügen über zwei Pfade zu jedem Netzwerk. Wenn eine Netzwerkkarte (oder deren Anschluss an das Interconnect-Modul) ausfällt, gibt es immer einen redundanten Pfad zum Switch-Netzwerk. Vom Ausfall einer Netzwerkkarte sind nur die Pakete betroffen, die zum Zeitpunkt des Ausfalls über die jeweilige Verbindung übertragen werden.

- Ausfall eines Scan-Blades

  Bei Ausfall eines Scan-Blades leitet der Management-Blade-Server den Scan-Datenverkehr automatisch an die verbleibenden Scan-Blades. Verbindungen zum Zeitpunkt des Ausfalls werden unterbrochen.

- Ausfall eines Management-Blade-Servers

  Bei Ausfall eines Management-Blade-Servers wird der Failover-Management-Blade-Server zum Master und setzt die Verteilung des Datenverkehrs an die Scan-Blades fort. Verbindungen zum Zeitpunkt des Ausfalls werden unterbrochen.

- Ausfall eines Interconnect-Moduls

  Dies wird ähnlich wie der Ausfall von internen und externen Verbindungen gehandhabt. Der gesamte Datenverkehr wird an und über das verbleibende Interconnect-Modul geleitet.

Entscheidung für die Verwendung des ausfallsicheren Modus

Überlegungen in Bezug auf den gewählten Bereitstellungsmodus an.

Im Standardmodus (nicht ausfallsicher) verwendet der McAfee Email Gateway Blade Server ein Interconnect-Modul für jedes LAN (LAN1 und LAN2), das für Ihren Blade-Server erforderlich ist.

Im ausfallsicheren Modus werden für jedes LAN zwei Interconnect-Module verwendet, sodass für LAN1 und LAN2 jeweils mehrere Netzwerkpfade aufgebaut werden können.

Den Blade-Server für den ausfallsicheren Modus einzurichten ist wesentlich komplexer als die Einrichtung des Standardmodus. Daher empfiehlt McAfee, den ausfallsicheren Modus nur dann zu verwenden, wenn Sie in der Lage sind, die erforderlichen Änderungen am Netzwerk und an anderen Komponenten vorzunehmen.

Falls Sie planen, auf Ihrem McAfee Email Gateway Blade Server den ausfallsicheren Modus zu verwenden, empfiehlt McAfee, Ihren Blade-Server zunächst im Standardmodus (nicht ausfallsicher) zu installieren, um sicherzustellen, dass der Blade-Server wie erwartet funktioniert.

Wenn alle Komponenten ordnungsgemäß arbeiten, konfigurieren Sie Ihren Blade-Server für den Betrieb im ausfallsicheren Modus um. In den folgenden Abschnitten werden die Schritte detailliert beschrieben, die für die Konfiguration Ihres Blade-Servers im Standardmodus (nicht ausfallsicher) notwendig sind. Im Anschluss wird erläutert, wie die notwendigen Änderungen für die Verwendung des ausfallsicheren Modus vorzunehmen sind, falls gewünscht.

Vor dem Umkonfigurieren in den ausfallsicheren Modus

Lernen Sie die Auswirkungen kennen, die die Neukonfiguration des Blade-Servers für den ausfallsicheren Modus haben kann.

McAfee empfiehlt, die unter *Planung Ihrer Installation* aufgeführten Informationen zu lesen und zu beachten, bevor Sie damit beginnen, Ihren McAfee Email Gateway Blade Server für den Betrieb im ausfallsicheren Modus umzukonfigurieren.

Hardware-Informationen

Lernen Sie die Hardware-Anforderungen für den ausfallsicheren Modus kennen.

Damit Ihre Hardware im ausfallsicheren Modus betrieben werden kann, muss Folgendes verfügbar sein:

- Eine Mindestanzahl an Blades

  Für den ausfallsicheren Modus wird mindestens benötigt:

  - Ein Management-Blade-Server
  - Ein Failover-Management-Blade-Server
  - Mindestens zwei Scan-Blades

- Eine ausreichende Anzahl von Netzwerkkarten in allen Blades

  Wenn Sie einen neuen McAfee Email Gateway Blade Server installieren, ist die gelieferte Hardware für den ausfallsicheren Modus geeignet.

  Wenn Sie jedoch einen bereits installierten McAfee Email Gateway Blade Server für den Betrieb im ausfallsicheren Modus umkonfigurieren, müssen Sie möglicherweise ein Upgrade der einzelnen Blades durchführen und Tochterkarten in den Blades installieren. Die Management- und Failover-Management-Blade-Server müssen in beiden Steckplätzen mit Tochterkarten gemäß McAfee-Spezifikationen ausgerüstet sein.

  Sie können in der Benutzeroberfläche des Onboard Administrator prüfen, ob diese Karten vorhanden sind. Prüfen Sie, ob Tochterkarten im Register "Information" der Anzeige "Device Bay" (Gerätefach) aufgeführt sind.

  Die Tochterkarten müssen vom richtigen Typ sein und sich in den richtigen Steckplätzen befinden. Dual-Port-Tochterkarten müssen im Fach 1 installiert sein, Quad-Port-Karten im Fach 2.

- Der Management-Blade-Server befindet sich im Blade-Fach 1 des Gehäuses.
- Der Failover-Management-Blade-Server befindet sich im Blade-Fach 2 des Gehäuses.
- Die Software McAfee Email Gateway steht zur Installation entweder auf einer CD-ROM, einem USB-Stick oder über den Onboard Administrator zur Verfügung.
- Interconnect-Module
  - Interconnect-Module des Typs HP GBe2c müssen in den Interconnect-Modul-Fächern 1 bis 4 installiert sein.

    Passthrough-Module müssen in den Interconnect-Modul-Fächern 5 und 6 installiert sein, um die OOB-Konnektivität zu ermöglichen.
- Module für den Onboard Administrator

  Redundante OA-Module müssen entsprechend den Anweisungen von HP installiert und konfiguriert sein.
- Stromversorgung

  Das Gehäuse muss mit ausreichenden Netzteilen gemäß den Empfehlungen in der HP-Dokumentation ausgestattet sein, um einen redundanten Betrieb für die vorgesehene Anzahl von Blades zu ermöglichen.

Für den ausfallsicheren Modus erforderliche IP-Adressen

Die Konfiguration Ihres Blade-Servers für den ausfallsicheren Modus erfordert, dass mehrere IP-Adressen erstellt werden.

Jedes Gehäuse benötigt IP-Adressen mindestens für folgende Elemente:

Tabelle 4-1 Ausfallsicherer Modus – IP-Adressen

Komponente	Gehäuse	Management-Blade-Server	Failover-Management-Blade-Server	Scan-Blades
Gehäuse-IP-Adressen				
Module für den Onboard Administrator	2			
Integrierte Lights-Out-Module (iLO) (1 pro Blade)	16			

Tabelle 4-1 Ausfallsicherer Modus – IP-Adressen *(Fortsetzung)*

Komponente	Gehäuse	Management-Blade-Server	Failover-Management-Blade-Server	Scan-Blades
Interconnect-Module (Switches)	4			
Modus "Expliziter Proxy"				
Physische IP-Schnittstelle 1		1 oder mehr	1 oder mehr	
Virtuelle (gemeinsame) IP-Schnittstelle 1		1 oder mehr		
Physische IP-Schnittstelle 2 (Optional)		1 oder mehr	1 oder mehr	
Virtuelle (gemeinsame) IP-Schnittstelle 2 (Optional)		1 oder mehr		
Modus "Transparenter Router"				
Physische IP-Schnittstelle 1		1 oder mehr	1 oder mehr	
Virtuelle (gemeinsame) IP-Schnittstelle 1		1 oder mehr		
Physische IP-Schnittstelle 2		1 oder mehr	1 oder mehr	
Virtuelle (gemeinsame) IP-Schnittstelle 2		1 oder mehr		
Modus "Transparente Bridge"				
Bridge-IP-Schnittstelle		1 oder mehr	1 oder mehr	
Virtuelle (gemeinsame) IP-Schnittstelle (Optional, beim Einrichten eines Proxy mit dieser virtuellen IP)		1 oder mehr		
Privates Scanning-Netzwerk				
Lastausgleichs-IP (Nur für das Gehäuse, nicht routbar, durch Management-/Failover-Management-Blades gesteuert, standardmäßig 169.254.1.0/24)		1	1	1 pro Blade-Server zum Scannen von Inhalten (Zugewiesen vom Management-Blade-Server)

Benutzernamen und Kennwörter

Informieren Sie sich über alle Benutzernamen und Kennwörter, die für die Konfiguration des ausfallsicheren Modus erforderlich sind.

Dieser Seite können Sie die Standardbenutzernamen und Kennwörter entnehmen, die von den diversen Komponenten innerhalb Ihres Blade-Servers verwendet werden.

Falls Sie Kennwörter oder Benutzernamen geändert haben, verwenden Sie diese anstelle der unten angegebenen Standardinformationen.

Tabelle 4-2 Benutzernamen und Kennwörter nach Komponente

Komponente	Standardbenutzername	Standardkennwort (bzw. Speicherort des Kennworts)
HP Onboard Administrator	Administrator	Siehe Aufkleber am Gehäuse
HP-Interconnect-Module	admin	admin
HP iLO	(verwaltet über den HP Onboard Administrator)	
Benutzeroberfläche der McAfee Email Gateway-Software	admin	Kennwort
Konsole der McAfee Email Gateway-Software	support	Kennwort

Aktivieren des ausfallsicheren Modus

Hier finden Sie eine Übersicht der Schritte, die durchgeführt werden müssen, um Ihre Blade-Server in den ausfallsicheren Modus zu versetzen.

Nachdem Sie Ihren McAfee Email Gateway Blade Server im Standardmodus (nicht ausfallsicher) installiert und konfiguriert haben, bietet Ihnen die folgende Tabelle einen Überblick über die Neukonfiguration des Blade-Servers im ausfallsicheren Modus.

McAfee empfiehlt, dass Sie den Blade-Server vor der Einrichtung im ausfallsicheren Modus zunächst im Standardmodus (nicht ausfallsicher) betriebsbereit konfigurieren.

Tabelle 4-3 Übersicht über die Installationsschritte für den ausfallsicheren Modus

Schritt	Beschreibung
1. Installieren und konfigurieren Sie den Blade-Server im Standardmodus (nicht ausfallsicher), und verifizieren Sie, dass er ordnungsgemäß läuft.	Standardinstallation auf Seite 28
2. Stellen Sie die erforderlichen Informationen über das Netzwerk zusammen.	Vor dem Umkonfigurieren in den ausfallsicheren Modus auf Seite 58 Hardware-Informationen auf Seite 58 Benutzernamen und Kennwörter auf Seite 60
3. Sichern Sie die vorhandene Konfiguration.	Sichern der vorhandenen Konfiguration
4. Erstellen Sie die Basiskonfiguration für die Interconnect-Module.	Konfigurieren der Interconnect-Module
5. Laden Sie die bearbeiteten Konfigurationsdateien hoch.	Anwenden der Konfiguration für den ausfallsicheren Modus auf alle Interconnect-Module
6. Laden Sie die generierten Konfigurationsdateien für die Interconnect-Module herunter, und überprüfen Sie sie.	Herunterladen und Überprüfen der generierten Konfiguration
7. Konfigurieren Sie den Management-Blade-Server für den ausfallsicheren Modus.	Konfigurieren des Management-Blade-Servers für die Verwendung des ausfallsicheren Modus

Tabelle 4-3 Übersicht über die Installationsschritte für den ausfallsicheren Modus

Schritt	Beschreibung
8. Nehmen Sie alle erforderlichen Änderungen an der Verkabelung des Blade-Servers vor.	Verbindungen zum externen Netzwerk im ausfallsicheren Modus
9. Schalten Sie die Blades ein.	Einschalten der Blades

Wenn Sie den Blade-Server an Ihr Netzwerk anschließen, können der Internetzugang oder andere Netzwerkdienste unterbrochen werden. Planen Sie einen Zeitraum ein, in dem das Netzwerk nicht verfügbar ist, vorzugsweise zu einer Zeit mit geringer Netzwerkauslastung.

Sichern der vorhandenen Konfiguration

Gehen Sie wie nachfolgend beschrieben vor, um die vorhandene Konfiguration Ihres McAfee Email Gateway Blade Server zu sichern.

McAfee empfiehlt, eine vollständige Sicherung Ihrer Blade-Server-Konfiguration zu erstellen, bevor Sie eine Aktualisierung durchführen, auch dann, wenn Sie vorhaben, eine der Aktualisierungsoptionen zu verwenden, die eine Sicherung und Wiederherstellung Ihrer Konfiguration einschließen.

Vorgehensweise

1 Navigieren Sie in der Benutzeroberfläche zu **System** | **Systemverwaltung** | **Konfigurationsverwaltung**.

2 Wählen Sie die optionalen Elemente aus, die Sie in die Sicherung aufnehmen möchten (versionsabhängig). McAfee empfiehlt, vor der Aktualisierung Ihres Blade-Servers alle Optionen zu sichern.

3 Klicken Sie auf **Konfiguration sichern**.

4 Nach kurzer Zeit wird ein Dialogfeld angezeigt, in dem Sie die gesicherte Konfigurationsdatei auf Ihren lokalen Computer herunterladen können.

Installieren der Interconnect-Module für den ausfallsicheren Modus

Bevor Sie Verbindungen aufbauen, müssen Sie die Ethernet-Interconnect-Module installieren und konfigurieren.

Tabelle 4-4 Legende zu den Abbildungen

#	Beschreibung
1	Anschlüsse für Stromversorgung
2	Interconnect-Module 1 und 2 (verbinden mit LAN 1)
3	Interconnect-Module 3 und 4 (verbinden mit LAN 2)
4	Onboard-Administrator-Anschluss
5	Onboard-Administrator-Modul
6	Out-of-Band-Zugang (Anschluss 20)
7	Out of Band (Passthrough)

Die Interconnect-Module werden an der Rückseite des Gehäuses direkt unter der oberen Kühllüfterreihe installiert.

Die Interconnect-Module für LAN 1 werden in die Interconnect-Modul-Fächer oben links und oben rechts eingesetzt, die Interconnect-Module für LAN 2 in die Interconnect-Modul-Fächer direkt darunter.

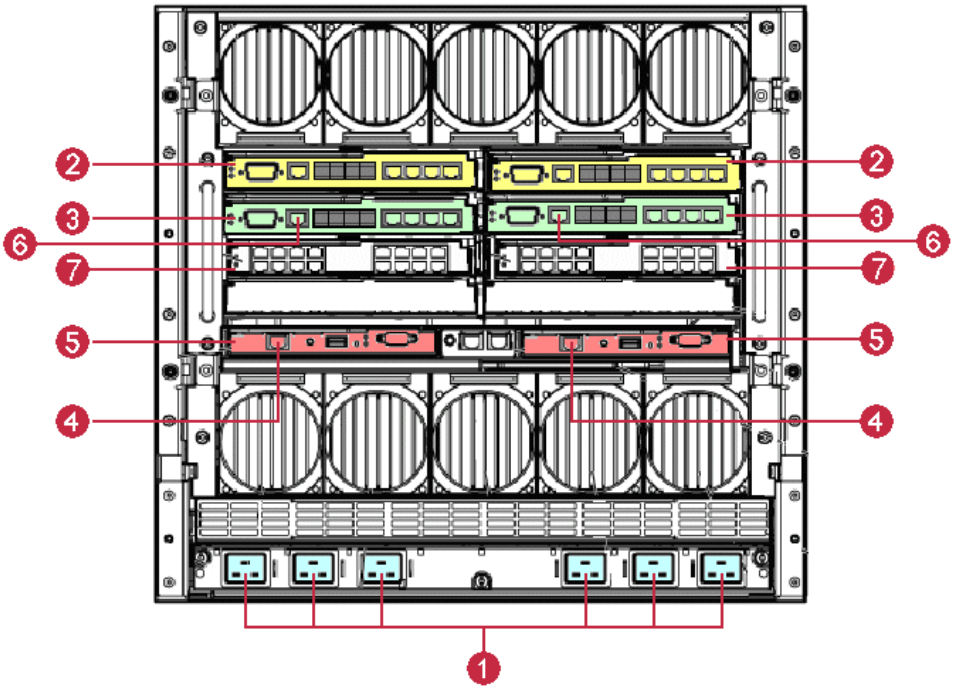


Abbildung 4-1 Positionen der Komponenten auf der Rückseite – Ausfallsicherer Modus

Führen Sie Folgendes aus:

- Stellen Sie sicher, dass der STP-Status (Spanning Tree Protocol) für die Spanning Tree Group 1 (STG1) „AUS" lautet – standardmäßig sind alle Anschlüsse Mitglieder von STG1. (Dies gilt, wenn Sie den Blade-Server im Modus „Transparente Bridge" installieren.)
- Konfigurieren Sie die ACLs (Access Control Lists, Zugriffssteuerungslisten) auf den Interconnect-Modulen so, dass die Blade-Server zum Scannen von Inhalten keine externen DHCP-Adressen empfangen können.
- Konfigurieren Sie die ACLs so, dass die Blade-Heartbeat-Pakete im Blade-Server verbleiben.
- Wenn für ein VLAN gekennzeichneter Datenverkehr durch den Blade-Server geleitet werden soll, müssen die Interconnect-Module so konfiguriert werden, dass sie diesen Datenverkehr durchlassen.

Informationen dazu, wie Sie dies tun, finden Sie in der unten aufgeführten Dokumentation:

- HP GbE2c Layer 2/3 Ethernet Blade Switch for c-Class BladeSystem Quick Setup
- HP GbE2c Layer 2/3 Ethernet Blade Switch for c-Class BladeSystem User Guide

In der Tabelle werden die verwendeten Interconnect-Module angezeigt. Standardmäßig können die externen Anschlüsse 21-24 von jedem Interconnect-Modul verwendet werden, um die Netzwerke anzuschließen.

Tabelle 4-5 Verwendung der Interconnect-Module

Interconnect-Modul-Fach	Standardmodus (nicht ausfallsicher)	Ausfallsicherer Modus
1	LAN1	LAN1, SCAN
2	Nicht verwendet	LAN1, SCAN
3	LAN2	LAN2, (OOB)

Tabelle 4-5 Verwendung der Interconnect-Module *(Fortsetzung)*

Interconnect-Modul-Fach	Standardmodus (nicht ausfallsicher)	Ausfallsicherer Modus
4	OOB	LAN2, (OOB)
5	OOB	OOB
6	Nicht verwendet	OOB
7	Nicht verwendet	Nicht verwendet
8	Nicht verwendet	Nicht verwendet

Beachten Sie Folgendes:

- Im Standardmodus (nicht ausfallsicher) wird das Scanning-Netzwerk direkt über LAN1 geleitet.
- Im Standardmodus (nicht ausfallsicher) schließen sich die aufgeführten Out-of-Band-Verbindungen (OOB) gegenseitig aus und sind auch nicht ausfallsicher.
- Im ausfallsicheren Modus nutzt das Scan-Netzwerk dieselben Netzwerkkarten wie LAN1, der Datenverkehr ist jedoch VLAN-gekennzeichnet, um das Scannen vom LAN1-Datenverkehr zu trennen.
- Im ausfallsicheren Modus ist das Scanning-Netzwerk auf den Scan-Blades ungekennzeichnet, um eine PXE-Installation der Scan-Blades zu ermöglichen.
- Die Interconnect-Modul-Fächer 5 und 6 werden von Passthrough-Modulen belegt, die eine direkte Verbindung mit den Management- und Failover-Management-Blade-Servern ermöglichen. Die Scan-Blades verfügen nicht über Out of Band-Verbindungen. Dies wird über die Management-Blade-Server und das Scanning-Netzwerk realisiert.
- Standardmäßig ist das Out-of-Band-VLAN als ungekennzeichnet und auf Anschluss 20 aller Interconnect-Module konfiguriert. Sie können Anschluss 20 der Interconnect-Module 1 und 2 verwenden, um mit Ihrem Out-of-Band-Netzwerk die Interconnect-Module des Gehäuses zu verwalten. Anschluss 20 der Interconnect-Module 3 und 4 sind für die Out-of-band-Verwaltung des McAfee Email Gateway Blade Server reserviert.

Bei Neuinstallationen und bei Upgrades, bei denen Sie Ihren Blade-Server für den ausfallsicheren Modus konfigurieren, hat sich der LAN2-Anschluss gegenüber früheren Versionen des McAfee Email Gateway Blade Server geändert. Bei Standard-Upgrades (nicht ausfallsicher) vorhandener Hardware wird das Interconnect-Modul 2 für den LAN2-Datenverkehr verwendet. Bei neuen Installationen oder bei Upgrades vorhandener Hardware für den ausfallsicheren Modus wird das Interconnect-Modul 3 für den LAN2-Datenverkehr verwendet.

Konfigurieren der Interconnect-Module

Die Interconnect-Module innerhalb des Blade-Servers müssen konfiguriert werden, damit das Gehäuse im ausfallsicheren Modus betrieben werden kann.

Die McAfee Email Gateway-Software übernimmt die Basiskonfigurationen für alle Interconnect-Module und verwendet sie zur automatischen Generierung der vollständigen Interconnect-Modul-Konfiguration, die für den Betrieb Ihres Blade-Servers im ausfallsicheren Modus benötigt wird.

Die Interconnect-Module innerhalb des Blade-Servers müssen konfiguriert werden, damit das Gehäuse im ausfallsicheren Modus betrieben werden kann.

Die McAfee Email Gateway-Software übernimmt die Basiskonfigurationen der Interconnect-Module und verwendet sie zur automatischen Generierung der vollständigen Interconnect-Modul-Konfiguration, die für den Betrieb Ihres Blade-Servers im ausfallsicheren Modus benötigt wird. Die Methode, mit der die automatisch generierte Konfiguration auf die Interconnect-Module angewendet wird, kann ausgewählt werden:

Tabelle 4-6 Konfigurationsmethoden

	Verantwortung	Anwendung der Interconnect-Modul-Konfiguration	Bereitgestellte Konfiguration
1.	Benutzer verwaltet Interconnect-Module	Konfigurationsinformationen werden kopiert und in die Interconnect-Modul-CLI eingefügt.	Keine Anmeldeinformationen in der Chassis-Konfiguration. Keine Basiskonfiguration für Interconnect-Module hochgeladen.
2.	Benutzer verwaltet Interconnect-Module	Konfiguration wird benutzergesteuert von der McAfee Email Gateway-Software oder einem externen FTP- bzw. TFTP-Server direkt in das Interconnect-Modul heruntergeladen.	Keine Anmeldeinformationen in der Chassis-Konfiguration. Basiskonfigurationsdateien für Interconnect-Module werden in die McAfee Email Gateway-Software hochgeladen.
3.	Benutzer verwaltet Interconnect-Module	Verwenden der Web-Benutzeroberfläche für Interconnect-Module zum Auffinden und Ändern der Konfiguration.	Keine Anmeldeinformationen in der Chassis-Konfiguration. Keine Basiskonfiguration für Interconnect-Module hochgeladen.
4.	Software verwaltet Interconnect-Module	Konfiguration wird bei jeder Änderung von der McAfee Email Gateway-Software direkt in die Interconnect-Module heruntergeladen.	Chassis-Konfiguration enthält Anmeldeinformationen für die Interconnect-Module. Basiskonfigurationsdateien für Interconnect-Module werden in die McAfee Email Gateway-Software hochgeladen.

Unter "Beispiel für die Basiskonfiguration eines Interconnect-Moduls" und "Beispiel einer Chassis-Konfigurationsdatei" finden Sie nähere Informationen dazu, welche Informationen in den Basiskonfigurationsdateien für die Interconnect-Modul- und Chassis-Konfigurationsdatei erforderlich sind.

Falls die McAfee Email Gateway-Software die Interconnect-Module automatisch konfigurieren soll, gehen Sie wie nachfolgend beschrieben vor, um Basiskonfigurationen für Interconnect-Module zu erstellen.

Das erforderliche Format für die Interconnect-Modul Basiskonfigurationsdateien ist vom Typ der eingebauten Interconnect-Module abhängig. Für HP GbE2c-Interconnect-Module müssen die Konfigurationsdateien im iscli-Format (wie Cisco IOS) und nicht im HP bladeos-cli-Format generiert werden.

Vorgehensweise

1. Laden Sie die gesamte Konfiguration von jedem Interconnect-Modul mittels FTP oder TFTP auf Ihre Workstation herunter, indem Sie sich bei der Web-Benutzeroberfläche jedes Interconnect-Moduls anmelden oder CLI verwenden.
2. Geben Sie für jedes Interconnect-Modul eindeutige Informationen an. Dazu gehören IP-Adressen, Route-Informationen, Syslog-Server, Zeitserver und Zeitzonen.
3. Entfernen Sie die Konfigurationseinträge für alle Anschlüsse, falls Sie nicht angegeben haben, dass diese Anschlüsse vom Konfigurationsgenerator für Interconnect-Module ignoriert werden sollen.

   Dies wird die Basiskonfiguration für jedes Interconnect-Modul.
4. Speichern Sie die Dateien unter /config/resiliency/interconnect.base.n (n = Interconnect-Modul-Nummer), und fügen Sie sie der gesicherten Konfigurations-ZIP-Datei hinzu.

Diese gesicherte Konfigurations-ZIP-Datei enthält auch die Datei "chassisconfig.xml", die unter "Ändern der Gehäusekonfiguration" beschrieben wird.

Ändern der Gehäusekonfiguration

Nehmen Sie die erforderlichen Änderungen an den Gehäusekonfigurationsdateien vor, indem Sie die Datei "chassisconfig.xml" ändern.

Die Datei "chassisconfig.xml" befindet sich innerhalb der Konfigurations-ZIP-Datei, die über **System** | **Systemverwaltung** | **Konfigurationsverwaltung** heruntergeladen werden kann.

Wenn Sie einen Management-Blade-Server das erste Mal installieren, wird eine standardmäßige Version der Datei "chassisconfig.xml" generiert.

Nachdem die Datei "chassisconfig.xml" aktualisiert wurde, wird die Interconnect-Modul-Konfiguration automatisch mit den Anschlusskonfigurationen des Blade-Interconnect-Moduls neu generiert.

Die Elemente innerhalb der Datei "chassisconfig.xml", die höchstwahrscheinlich geändert werden müssen, damit sie Ihren Netzwerkanforderungen entsprechen, sind folgende:

- ScanningVlan (Standard 4094)

  Dies ist die VLAN-ID, die innerhalb des Chassis für das Scanning-Netzwerk verwendet wird.

  Unter normalen Umständen ist dieses VLAN an den externen Anschlüssen des Interconnect-Moduls nicht sichtbar.

  Dieses Netzwerk kann über den symbolischen Namen "scan" an Anschlüsse gebunden werden.
- UntaggedVlan (Standard 4093)

  Dies ist die VLAN-ID, die innerhalb des Chassis für den Transport ungekennzeichneter Rahmen zum externen Netzwerk verwendet wird.

  Dieses Netzwerk kann über den symbolischen Namen "defuntagged" an Anschlüsse gebunden werden.

  Dieses VLAN wird nur innerhalb der Interconnect-Module verwendet. Für den Management-Blade-Server bestimmter Datenverkehr wird mit denselben Tags gekennzeichnet, die auch bei externen Verbindungen vorhanden sind.

- OobVlan (Standard 4092)

  Dies ist die VLAN-ID, die innerhalb des Chassis für die Trennung des OOB-Netzwerks von den anderen Netzwerken innerhalb des Chassis verwendet wird.

  Dieses Netzwerk kann über den symbolischen Namen "oob" an Anschlüsse gebunden werden.

- BridgeVlan (kein Standardwert)

  Dies ist eine Liste der VLANs, die im Modus "Transparente Bridge" von LAN1 nach LAN2 überbrückt werden. Es ist nicht erforderlich, VLANs anzugeben, die im

  McAfee Email Gateway-Modus "Transparente Bridge" für das Scannen ausgewählt wurden, da diese automatisch hinzugefügt werden. Die hier angegebenen VLANs werden nicht gescannt, sondern nur von LAN1 nach LAN2 überbrückt.

  Dieses Element wird nur dann verwendet, wenn das System im Modus "Transparente Bridge" betrieben wird. Die Liste der externen VLANs kann über den symbolischen Namen "external" referenziert werden.

- ScanningSTG/ExternalSTG/OobStg

  Dies sind die Konfigurationen für die Spanning-Tree-Gruppen, die für den jeweiligen Spanning Tree des Scanning-Netzwerks, des externen Netzwerks und des OOB-Netzwerks verwendet werden.

  Je nach Topologie des externen Netzwerks und der STG-Konfiguration kann es erforderlich sein, das jeweilige Prioritätsfeld zu ändern.

- Blades

  In diesem Abschnitt sind die Funktionen der einzelnen Blade-Steckplätze aufgeführt. Ein Steckplatz kann als Management-Blade-Server (für den Fall, dass sich die Management-Blade-Server nicht in den Steckplätzen 1 und 2 befinden) oder als zu ignorierender Steckplatz konfiguriert werden. Wenn ein Steckplatz als zu ignorierend konfiguriert wird, wird für die an das Blade angeschlossenen Interconnect-Modul-Anschlüsse keine Konfiguration generiert.

- • Interconnect-Modul-Anmeldeinformationen

  Falls es erforderlich ist, dass die Interconnect-Module ihre Konfiguration automatisch von der McAfee Email Gateway-Software erhalten, müssen diese Anmeldeinformationen die richtige IP-Adresse, den richtigen Benutzernamen und das richtige Kennwort enthalten.

  Beachten Sie, dass diese Anmeldeinformationen im Klartext gespeichert werden und daher gelesen werden können, falls das McAfee Email Gateway-System kompromittiert werden sollte.

- Interconnect Ports

  Der Betriebsmodus der Interconnect-Modul-Anschlüsse kann hier festgelegt werden. Der wahrscheinlichste Grund zur Änderung der Einstellungen der Interconnect-Modul-Anschlüsse ist es, LACP für die externen Anschlüsse zu aktivieren oder zu deaktivieren oder STP zu aktivieren oder zu deaktivieren. Eine Änderung der Anschlusseinstellungen kann auch erforderlich sein, um externe Anschlüsse für das Scanning-Netzwerk zu reservieren.

  Das VLAN, über das ungekennzeichnete Rahmen die Anschlüsse passieren, wird hier definiert.

  Es kann hilfreich sein, den Anschlüssen aussagekräftige Namen zuzuweisen, wenn die von der McAfee Email Gateway-Software zugewiesenen Namen nicht ausreichend sind.

  Es kann auch angegeben werden, welche Anschlüsse vom Konfigurationsgenerator der McAfee Email Gateway-Software ignoriert werden sollen. Dies verursacht jedoch eine Fehlermeldung, wenn der Konfigurationsgenerator der McAfee Email Gateway-Software eine Konfiguration auf den betreffenden Anschluss einer der Blade-Steckplätze übernehmen muss.

- Interconnect-VLANs

  Die Zugehörigkeit der Interconnect-Modul-Anschlüsse zu den VLANs wird hier definiert. VLAN-IDs können numerisch oder – bei den VLANs des McAfee Email Gateway – über die oben genannten Namen symbolisch referenziert werden.

Des Weiteren kann in Erwägung gezogen werden, Folgendes zu konfigurieren:

- das Trunking der externen Interconnect-Modul-Anschlüsse
- die Spanning-Tree-Einstellungen
- der Zugriff auf Ihre Out-of-Band-Management-Netzwerke

In dem Sie die Interconnect-Modul-Anmeldeinformationen und IP-Adressen in die Datei "chassisconfig.xml" aufnehmen, kann die McAfee Email Gateway-Software die Konfigurationen automatisch auf die Interconnect-Module übernehmen.

McAfee empfiehlt jedoch, dies erst zu tun, nachdem Sie verifiziert haben, dass die automatisch generierte Konfiguration ordnungsgemäß funktioniert.

Anwenden der Konfiguration für den ausfallsicheren Modus auf alle Interconnect-Module

Wenden Sie die Konfiguration für den ausfallsicheren Modus auf die Interconnect-Module an.

Wie in Ändern der Gehäusekonfiguration auf Seite 66 dargestellt, empfiehlt McAfee, die Interconnect-Modul-IP und die Anmeldeinformationen erst dann in die Konfigurationsdateien einzutragen, wenn Sie die Dateien hochgeladen und geprüft haben, ob die enthaltenen Informationen korrekt sind.

Auf diese Weise wird vermieden, dass die Interconnect-Module mit fehlerhaften Informationen konfiguriert werden.

Wenn die Konfigurationsdateien korrekt sind, können Sie die Interconnect-Modul-IP und die Anmeldeinformationen hinzufügen und erneut hochladen. Anschließend werden die Konfigurationsdateien auf die Interconnect-Module angewendet.

Laden Sie die geänderten Konfigurationsdateien auf den Management-Blade-Server, indem Sie eine Konfigurations-ZIP-Datei mit allen geänderten Dateien erstellen und anschließend diese Datei über **System** | **Systemverwaltung** | **Konfigurationsverwaltung** wiederherstellen. Dazu gehören:

- Alle Basiskonfigurationsdateien für Interconnect-Module.
- Die Datei "chassisconfig.xml".

Sie müssen die Änderungen übernehmen, damit der Blade-Server die hochgeladene Konfiguration verwenden kann.

Falls Sie die Anmeldeinformationen und IP-Adressen für Interconnect-Module in die Gehäusekonfigurationsdatei (chassisconfig.xml) aufgenommen haben, wird die Konfiguration für den ausfallsicheren Modus automatisch auf jedes Interconnect-Modul angewendet.

Herunterladen und Überprüfen der generierten Konfiguration

Laden Sie die generierten Konfigurationsdateien "interconnect_config.X.n" herunter, und überprüfen Sie sie.

Vergewissern Sie sich, dass die generierte Konfiguration der gewünschten Konfiguration entspricht.

Diese werden unter **System** | **Systemverwaltung** | **Cluster-Verwaltung** | **Ausfallsicherer Modus** angezeigt.

Sollten diese Dateien fehlerhaft sein, wiederholen Sie die Schritte zum Definieren und Generieren der Konfiguration, um diese Probleme zu beheben.

Konfigurieren des Management-Blade-Servers für den ausfallsicheren Modus

Konfigurieren Sie den Management-Blade-Server für den ausfallsicheren Modus.

Vorgehensweise

1. Navigieren Sie in der Benutzeroberfläche zu **System** | **Systemverwaltung** | **Cluster-Verwaltung** | **Ausfallsicherer Modus**.
2. Klicken Sie auf **Ausfallsicheren Modus aktivieren**.
3. Klicken Sie zur Bestätigung, dass Sie die **Warnung beim Aktivieren des ausfallsicheren Modus** verstanden haben, auf **OK**.
4. Warten Sie darauf, dass der Management-Blade-Server, der Failover-Management-Blade-Server und alle Scan-Blades automatisch herunterfahren.
5. Nehmen Sie alle erforderlichen Änderungen an den Interconnect-Modulen für die Verbindung eines externen Netzwerkes mit den Blade-Servern vor.
6. Schließen Sie den Management-Blade-Server und den Failover-Management-Blade-Server an die Stromversorgung an.

   Überprüfen Sie im **Dashboard**, ob der Management- und der Failover-Management-Blade-Server ordnungsgemäß funktionieren und ob die Synchronisierung stattgefunden hat.
7. Schalten Sie der Reihe nach alle Blade-Server zum Scannen von Inhalten ein.

Verbindungen zum externen Netzwerk im ausfallsicheren Modus

Konfigurieren Sie die Verbindungen, die Sie zwischen Ihrem externen Netzwerk und Ihrem McAfee Email Gateway Blade Server benötigen.

Die Verbindungen, die Sie zwischen Ihrem externen Netzwerk und Ihrem McAfee Email Gateway Blade Server benötigen, hängen vom Betriebsmodus ab, den Sie für den Blade-Server ausgewählt haben, sowie von der Konfiguration des externen Netzwerks.

Wenn Sie den Onboard Administrator (OA) verwenden, stellen Sie sicher, dass Sie Verbindungen zum OA sowie zu den Interconnect-Modulen haben.

Stellen Sie sicher, dass alle Verbindungen zwischen dem Netzwerk und den Interconnect-Modulen des Blade-Servers aus gebündelten Verbindungen bestehen, um Ausfallsicherheit für den Fall zu bieten, dass ein Switch, ein Interconnect-Modul oder ein Kabel ausfällt.

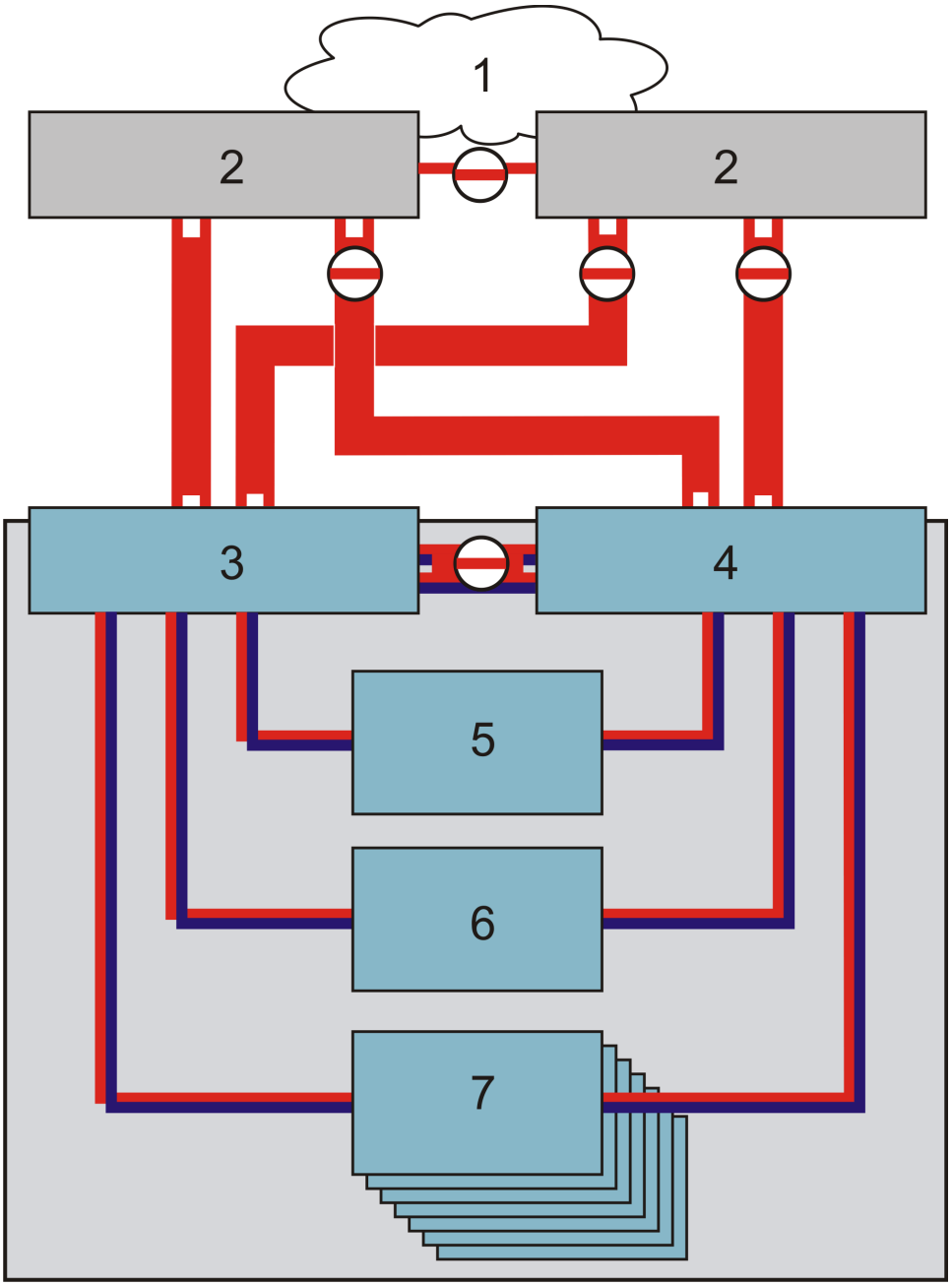


Abbildung 4-2 Typische Netzwerkverbindungen - ausfallsicherer Modus

Tabelle 4-7 Schlüssel

	LAN-Verbindungen (LAN1, LAN2 oder OOB)
	Internes Scanning-Netzwerk
	Gebündelte Verbindungen

Tabelle 4-7 Schlüssel *(Fortsetzung)*

	Von STP normalerweise blockierte Verbindungen
1.	Externes Netzwerk
2.	Netzwerkinfrastruktur
3.	(für LAN1) Interconnect-Modul 1, (für LAN2 oder OOB) Interconnect-Modul 3
4.	(für LAN1) Interconnect-Modul 2, (für LAN2 oder OOB) Interconnect-Modul 4
5.	Management-Blade-Server
6.	Failover-Management-Blade-Server
7.	Scan-Blades

Zwecks einfacherer Darstellungen wird im Diagramm nur ein Satz von LAN/OOB-Pfaden gezeigt. Die Pfade für LAN1, LAN2 und OOB sind ähnlich.

Einschalten der Blades

Schließen Sie alle Blades in Ihrem McAfee Email Gateway Blade Server an die Stromversorgung an.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie alle unter Aktivieren des ausfallsicheren Modus auf Seite 61 beschriebenen Aufgaben erfüllt haben.

Vorgehensweise

1. Drücken Sie die Netzschalter am Management-Blade-Server.
2. Wenn der Management-Blade-Server die Startsequenz abgeschlossen hat, drücken Sie den Netzschalter des Failover-Management-Blade-Servers.
3. Nachdem der Management-Blade-Server und Failover-Management-Blade-Server ihre Startsequenzen abgeschlossen haben, können Sie die Blade-Server zum Scannen von Inhalten einschalten.

Zur Vermeidung von Spannungsspitzen empfiehlt McAfee, dass Sie warten, bis jedes Scan-Blade die Startsequenz abgeschlossen hat, bevor Sie den nächsten Blade-Server zum Scannen von Inhalten einschalten.

5 Fehlerbehebung

Hier finden Sie die Beschreibung von Problemen, die beim Integrieren Ihres Geräts in das bereits vorhandene Netzwerk auftreten können.

Für die Verwendung des Tools zur Fehlerbehebung, das in der Benutzeroberfläche der McAfee Email Gateway Appliance-Software zur Verfügung steht, wählen Sie in der Navigationsleiste **Fehlerbehebung** aus.

Blade-spezifische Fehlerbehebung

Hier finden Sie spezifische Informationen für die Fehlerbehebung bei Ihrem McAfee Email Gateway Blade Server.

Externe Überwachungssysteme

McAfee empfiehlt, ein dediziertes Überwachungssystem zu konfigurieren, das zusätzliche Warnungen zu Problemen oder Fehlern innerhalb der McAfee Email Gateway Blade Server-Gehäuse liefert.

Der Zustand des Gehäuses und der Interconnect-Module kann mithilfe des Simple Network Management Protocol (SNMP) direkt überwacht werden. Außerdem können die integrierten Lights-Out-Module so konfiguriert werden, dass sie SNMP-Traps senden, falls Fehlerzustände festgestellt werden. Die McAfee Email Gateway Blade Server-Software kann auch über SNMP überwacht werden.

Status der Netzwerkkarte

Erfahren Sie, wo Sie den Status der Netzwerkkarten überprüfen können.

Der Status der Verbindungen zu allen Netzwerkkarten auf jedem Blade ist über die Benutzeroberfläche der McAfee Email Gateway -Software unter **System** | **Systemverwaltung** | **Cluster-Verwaltung** verfügbar.

Systemereignisse

Erfahren Sie, wo Systemereignisse angezeigt werden.

Verwenden Sie **Berichte** | **Systemberichte** innerhalb der Benutzeroberfläche der McAfee Email Gateway-Software, um Informationen des Blade-Überwachungssystems und des Konfigurationssystems für die Interconnect-Module abzurufen.

A Anhänge

Hier finden Sie nützliche Informationen für die Installation und Konfiguration Ihres Blade-Servers.

Inhalt

- *Beispiel für die Basiskonfiguration eines Interconnect-Moduls*
- *Beispiel einer Chassis-Konfigurationsdatei*
- *Prozeduren für den Hardware-Austausch*

Beispiel für die Basiskonfiguration eines Interconnect-Moduls

Hier finden Sie ein Beispiel der Basiskonfiguration für eines der Interconnect-Module in Ihrem Blade-Server.

Wenn Sie Ihren McAfee Email Gateway Blade Server für die Verwendung des ausfallsicheren Modus konfigurieren, wird für jedes Interconnect-Modul in Ihrem Blade-Server-Gehäuse eine Basiskonfigurationsdatei benötigt.

Beispiel für die Basiskonfiguration eines Interconnect-Moduls – interconnect_base.n (n = Interconnect-Modul-Nummer)

```
version "5.1.3"
switch-type "GbE2c L2/L3 Ethernet Blade Switch for HP c-Class BladeSystem"
!
!
!
no system bootp
hostname "sw1"
system idle 60
!
ip dns primary-server 10.9.9.1
!
ntp enable
ntp primary-server 10.9.9.1
ntp interval 60
!
system timezone 180
! Europe/Britain/GB
system daylight
!
!
!
access user administrator-password
"ebfec37e832a822ab6b7a2b7409a21d800e2b27007bb4b41b7dd3b7827e7ec0f"
!
!
!
!
```

Beispiel einer Chassis-Konfigurationsdatei

Hier finden Sie ein Beispiel für die Chassis-Konfigurationsdatei eines Blade-Servers, der im ausfallsicheren Modus betrieben wird.

Beispiel mit einem Ausschnitt der Datei "chassisconfig.xml" für das Interconnect-Modul mit ID="1"

```
<!-- Copyright (C) 2010 McAfee Inc. All rights reserved. -->

<!-- default configuration layout for EWS usage of the C3000 chassis -->
<!-- this gets merged with the operational requirements based on configuration
-->


<Chassis>
    <Chassis>
        <!-- there are no default credentials since they are different per
chassis -->
        <!-- <OnBoardAdmin username="Administrator" password="password"/> -->

        <!-- the vlan we use for our scanning network -->
        <ScanningVlan vlanTag="4094"/>

        <!-- the vlan we use for external untagged traffic within the chassis --
>
        <UntaggedVlan vlanTag="4093"/>

        <!-- the vlan we use for our OOB network -->
        <OobVlan      vlanTag="4092"/>

        <!-- additional external tagged VLANs that need to be bridged through
from lan1 to lan2 -->
        <!-- <BridgeVlan> <VlanTag vlanTag="1234"/> </BridgeVlan> -->
        <BridgeVlan/>

        <!-- STG definitions for the above -->
        <ScanningSTG id="127" priority="32768" enable="yes"/>
        <ExternalSTG id="1" priority="32767" enable="yes"/>
        <OobSTG id="126" priority="32768" enable="yes"/>
    </Chassis>

    <Networks>
        <!-- the resiliency configuration for the bonded pairs of links -->
        <!-- the lan1/lan2 settings are ignored in transparent bridge mode since
STP is used instead -->
        <!-- we have to automatically calculate the arpTargets for each LAN as
the links are bought up -->
        <Network id="lan1" bond_mode="balance-alb"/>
        <Network id="lan2" bond_mode="balance-alb"/>
        <Network id="scan" bond_mode="balance-alb"/>
        <Network id="oob"  bond_mode="active-backup"/>
```

```
    </Networks>

    <Blades>
        <!-- default topology is that blades 1 and 2 are the management blades
-->
        <Blade id="1" isMgmt="yes"/>
        <Blade id="2" isMgmt="yes"/>
        <!-- this is how to ignore a blade slot completely -->
        <!-- <Blade id="3" ignore="yes"/> -->
    </Blades>

    <Interconnects>
        <Interconnect id="1">
            <!-- Add ip="a.b.c.d" to the credentials node to allow the system to
automatically configure the interconnects -->
            <Credentials username="admin" password="admin" ip="1.2.3.4"/>
            <!-- cross connects -->
            <Ports>
                <!-- Permitted attributes for the Port element are: -->
                <!-- id = the port number -->
                <!-- name = textual label for use in UI and SNMP etc. -->
                <!-- vlanId = 1-4095, the VLAN used for untagged frames on this
port -->
                <!-- enable = yes/no -->
                <!-- edgePort = yes/no, is this an edge port as far as STP is
concerned -->
                <!-- lacpEnable = active/passive/off -->
                <!-- lacpKey = LACP group to identify ports trunked to the same
peer -->
                <!-- lacpPriority = 0-65535, priority for the port within the
LACP group -->
                <!-- stpEnable = yes/no, is STP enabled on this port or not -->
                <!-- ignore = yes/no, if yes then no config will be generated
for this port -->

                <!-- cross connects -->
                <Port id="17" name="CrossConnectAto2" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="100" stpEnable="yes"/>
                <Port id="18" name="CrossConnectBto2" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="100" stpEnable="yes"/>

                <!-- internal chassis management network port - we can't change
this-->
                <Port id="19" ignore="yes"/>

                <!-- external ports -->
                <Port id="20" name="External20" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="101" stpEnable="yes"/>
                <Port id="21" name="External21" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="101" stpEnable="yes"/>
                <Port id="22" name="External22" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="101" stpEnable="yes"/>
                <Port id="23" name="External23" vlanId="defuntagged"
enable="yes" edgePort="no" lacpEnable="active" lacpKey="101" stpEnable="yes"/>
                <Port id="24" name="External24" vlanId="defuntagged"
```

```
enable="yes" edgePort="no" lacpEnable="active" lacpKey="101" stpEnable="yes"/>
            </Ports>

            <VLANs>
                <!-- Permitted attributes for the VLAN elements are: -->
                <!-- id = 1-4095, VLAN ID -->
                <!-- name = textual name for UI and SNMP etc. use -->
                <!-- stgId = 1-127, spanning tree group for the VLAN -->
                <!-- The ports which are in the VLAN are defined within the VLAN
element -->

                <!-- VLAN for OOB traffic -->
                <!-- blade port bindings are added automatically -->
                <VLAN id="oob"/>

                <!-- VLAN for internal scanning network -->
                <!-- blade port bindings are added automatically -->
                <VLAN id="scan">
                    <Port id="17"/>
                    <Port id="18"/>
                </VLAN>

                <!-- VLAN(s) for external traffic -->
                <!-- blade port bindings are added automatically -->
                <VLAN id="external" stgId="1">
                    <Port id="17"/>
                    <Port id="18"/>
                    <Port id="20"/>
                    <Port id="21"/>
                    <Port id="22"/>
                    <Port id="23"/>
                    <Port id="24"/>
                </VLAN>
            </VLANs>

        </Interconnect>

    </Interconnects>


</Chassis>
```

Prozeduren für den Hardware-Austausch

Erfahren Sie, wie Sie beim Austausch fehlerhafter Hardware-Komponenten vorgehen müssen.

Ersetzen eines ausgefallenen Management-Blade-Servers

Ersetzen Sie einen ausgefallenen Management-Blade-Server.

Gehen Sie wie nachfolgend beschrieben vor, um einen ausgefallenen Management-Blade-Server zu ersetzen.

Vorgehensweise

1. Fahren Sie den Management-Blade-Server herunter.
2. Entfernen Sie den alten Management-Blade-Server.
3. Setzen Sie den neuen Management-Blade-Server ein.

4 Installieren Sie die McAfee Email Gateway-Software.

   Weitere Informationen über die Neuinstallation der Software und die Konfiguration des Management-Blade-Servers finden Sie unter Installieren der Software auf Seite 34.

5 Konfigurieren Sie das neue Blade als Management-Blade-Server (sofern erforderlich).

Ersetzen eines ausgefallenen Failover-Management-Blade-Servers

Ersetzen Sie einen ausgefallenen Failover-Management-Blade-Server.

Gehen Sie wie nachfolgend beschrieben vor, um einen ausgefallenen Failover-Management-Blade-Server zu ersetzen.

Vorgehensweise

1 Fahren Sie den Failover-Management-Blade-Server herunter.

2 Entfernen Sie den alten Failover-Management-Blade-Server.

3 Setzen Sie den neuen Failover-Management-Blade-Server ein.

4 Installieren Sie die McAfee Email Gateway-Software.

   Weitere Informationen über die Neuinstallation der Software und die Konfiguration des Failover-Management-Blade-Servers finden Sie unter Installieren der Software auf Seite 34.

5 Konfigurieren Sie das neue Blade als Failover-Management-Blade-Server (sofern erforderlich).

Ersetzen eines ausgefallenen Blade-Servers zum Scannen von Inhalten

Ersetzen Sie einen ausgefallenen Blade-Servers zum Scannen von Inhalten.

Falls das neue Blade leere Festplatten hat, wird automatisch ein Scan-Blade-Image installiert. Anderenfalls folgen Sie den Anweisungen unter "Installieren der Software auf einem Blade-Server zum Scannen von Inhalten", um den Blade-Server zum Scannen von Inhalten zu zwingen, seine Software neu zu installieren.

Vorgehensweise

1 Fahren Sie das Blade herunter.

   Warten Sie darauf, dass sich das Blade ausschaltet.

2 Ersetzen Sie das Blade, nachdem es sich ausgeschaltet hat.

Ersetzen eines ausgefallenen Interconnect-Moduls

Ersetzen Sie ein ausgefallenes Interconnect-Modul.

Zum Ersetzen eines ausgefallenen Interconnect-Moduls ist es erforderlich, entweder eine Systemstillstandszeit einzuplanen, um das Ersatz-Interconnect-Modul vor Ort zu konfigurieren, oder das Interconnect-Modul in einem zweiten Blade-Server getrennt vom Produktionssystem zu konfigurieren.

Das Ersatz-Interconnect-Modul muss offline konfiguriert werden, da die Standardkonfiguration die laufende Netzwerktopologie beeinträchtigen könnte.

So ersetzen Sie ein Interconnect-Modul, wenn kein Reserve-Blade-Server verfügbar ist:

Vorgehensweise

1. Fahren Sie alle Scan-Blades herunter.
2. Fahren Sie den Failover-Management-Blade-Server herunter.
3. Laden Sie die Konfigurationsdatei für das Interconnect-Modul vom Management-Blade-Server herunter (falls die McAfee Email Gateway-Software das Interconnect-Modul nicht automatisch konfigurieren darf).
4. Trennen Sie das Chassis von allen Netzwerken mit Ausnahme des OOB-Netzwerks (wenn Sie die Interconnect-Module 1 oder 2 ersetzen) oder des LAN1-Netzwerks (wenn Sie die Interconnect-Module 3 oder 4 ersetzen), so dass nur noch ein Interconnect-Modul mit dem verbleibenden LAN verbunden ist.
5. Ersetzen Sie das Interconnect-Modul, und schalten Sie es ein.
6. Stellen Sie sicher, dass das Interconnect-Modul eine geeignete IP-Adresse. Dies sollte automatisch der Fall sein, wenn das Interconnect-Modul seine IP-Adresse über DHCP und das OA-Modul bezieht.
7. Wenn die McAfee Email Gateway-Software das Interconnect-Modul nicht automatisch konfigurieren darf, laden Sie die Konfiguration des Interconnect-Moduls hoch.

   Wenn die McAfee Email Gateway-Software das Interconnect-Modul automatisch konfigurieren darf, verwenden Sie die Schaltfläche "Interconnect-Modul-Konfiguration übernehmen" der grafischen Benutzeroberfläche von McAfee Email Gateway, oder geben Sie in der Textkonsole des Management-Blade-Servers folgenden Befehl ein: scm/opt/NETAwss/resiliency/apply_chassis_config.
8. Verifizieren Sie, dass das Interconnect-Modul die Konfiguration ohne Fehler angenommen hat.
9. Stellen Sie die Netzwerkverbindungen wieder her.
10. Schalten Sie den Failover-Blade-Server und die Scan-Blades wieder ein.

Ersetzen eines ausgefallenen Onboard-Administrator-Moduls

Ersetzen Sie ein ausgefallenes Onboard-Administrator-Modul.

Die korrekte Vorgehensweise beim Austausch des Onboard-Administrator-Moduls finden Sie in der HP-Dokumentation.

Index

A

Assistent "Benutzerdefinierte Einrichtung" 37
Ausfallsicher (Modus) 55

B

Bedrohungs-Feedback 39
Betriebsmodi
    Expliziter Proxy (Modus) 17
    Modus „Transparenter Router“ 15
    Transparente Bridge (Modus) 12
Bridge-Priorität 14

C

Cluster-Konfiguration
    Statistiken 39

D

Dashboard 39
Demilitarisierte Zone (DMZ) 19
DHCP 36
Diagramme
    E-Mail- und Netzwerkstatistiken 39
DMZ 19
    SMTP-Konfiguration 19
Dokumentation
    Produktspezifisch, suchen 7
    Typografische Konventionen und Symbole 5
    Zielgruppe dieses Handbuches 5

E

E-Mail-Gateway
    Mit einer DMZ (entmilitarisierten Zone) 19
E-Mail-Relay
    In einer DMZ (entmilitarisierte Zone) 19
E-Mail-Status 39
E-Mail-Warteschlangen 39
Entmilitarisierte Zone
    SMTP-Konfiguration 19
Erkennungen
    Raten und Statistiken 39
Expliziter Proxy (Modus) 17

F

Firewall-Regeln
    Expliziter Proxy (Modus) 17

H

Handbuch, Informationen 5

I

Installationsoptionen
    Benutzerdefinierte Einrichtung 37

K

Konfigurationskonsole 36
Konventionen und Symbole in diesem Handbuch 5

M

McAfee Global Threat Intelligence 39
McAfee ServicePortal, Zugriff 7
Meldungen beim Ändern der Konfiguration 39
Modus „Transparenter Router“ 15

N

Netzwerkmodi
    Einführung 11
    Expliziter Proxy (Modus) 17
    Modus „Transparenter Router“ 15
    Transparente Bridge (Modus) 12
Netzwerkstatus 39

R

Richtlinien
    Status 39

S

ServicePortal, Quellen für Produktinformationen 7
Setup-Assistent
    Benutzerdefiniert 37
Statistiken
    Dashboard 39
STP 14

T

Technischer Support, Produktinformationen suchen 7
Transparente Bridge (Modus) 12

W

Warnmeldungen
    Dashboard 39

McAfee
An Intel Company